Determination of the Structure of all Linear Homogeneous Groups in a Galois Field which are Defined by a Quadratic Invariant.

By Leonard Eugene Dickson.

Following the study of certain classes of finite linear groups defined by a quadratic invariant, it seems desirable to have a complete determination of this important type of groups. Besides the work of Jordan* on the two hypoabelian groups in the field of integers taken modulo 2, and the writer's generalization† of the first hypoabelian group to the Galois field of order 2^n, the structures of the orthogonal group‡ on m indices in the Galois field of order p^n (aside from certain low values of m, n, p) and of the group|| in the same field, leaving invariant the quadratic form $\sum_{i=1}^{m} \xi_i \eta_i$, have been previously determined by the writer.

By setting up a complete set of canonical forms for quadratic forms in m variables in every Galois field, we are able to prove that there exist but two new distinct types of groups defined by a quadratic invariant, one of these being a generalization of the second hypoabelian group of Jordan. Two new systems of simple groups are thus obtained [see §56]. The investigation completes and correlates the results of the earlier papers. It has been the aim throughout to devise

* Traité des Substitutions, pp. 195–213 and p. 440.

† "On the First Hypoabelian Group Generalized," The Quarterly Journal, pp. 1–16, 1898; "The Structure of the Hypoabelian Groups," Bulletin of the American Mathematical Society, pp. 495–510 July, 1898.

‡ "Systems of Simple Groups derived from the Orthogonal Group," Proceedings of the California Academy of Sciences, vol. I, No. 4, 1898, and No. 5, 1899; also Bulletin of the Amer. Math. Society, Feb., 1898, and May, 1898.

|| "The Structure of Certain Linear Groups with Quadratic Invariants," Proceedings of the London Mathematical Society, vol. XXX, pp. 70–98.

methods which require as few separations into cases and special treatments of lower cases as possible. The earlier methods for the orthogonal group have been abandoned in the main.

1. Consider a quadratic function ϕ homogeneous in m variables $\xi_1, \xi_2, \ldots, \xi_m$ and having as coefficients marks* of the Galois field of order p^n. We restrict ourselves to forms ϕ of determinant not zero in the $GF[p^n]$ and suppose, for the present, that $p > 2$. By an investigation analogous to that in Bachmann, Zahlentheorie, IV, pp. 409–412, we can prove that there exists a linear homogeneous substitution T on the variables $\xi_1, \ldots, \xi_m$ with coefficients belonging to the $GF[p^n]$ which transforms ϕ into

$$f_s \equiv \sum_{i=1}^{s} \xi_i^2 + \nu \sum_{i=s+1}^{m} \xi_i^2,$$

ν denoting any particular not-square in the $GF[p^n]$. Further, we can transform f_s into f_{s+2}. Consider indeed the substitution of determinant $\alpha^2 + \beta^2$,

$$\xi_i' = \alpha\xi_i - \beta\xi_j, \quad \xi_j' = \beta\xi_i + \alpha\xi_j.$$

It transforms $\xi_i^2 + \xi_j^2$ into $(\alpha^2 + \beta^2)(\xi_i^2 + \xi_j^2)$. By the theorem quoted in §3, there exist marks α, β in the $GF[p^n]$, $p > 2$, for which $\alpha^2 + \beta^2 = \nu$, a not-square. Hence in the form f_s we can replace $\xi_i^2 + \xi_j^2$ by $\nu\xi_i^2 + \nu\xi_j^2$ and inversely. We have therefore two canonical forms, f_m and f_{m-1}.

For m odd, the form f_{m-1} can be transformed into

$$f_0 \equiv \nu(\xi_1^2 + \xi_2^2 + \ldots + \xi_m^2).$$

But the group leaving f_0 invariant leaves also $f_m \equiv \xi_1^2 + \ldots + \xi_m^2$ invariant. We may therefore state the result:

Theorem: *Every linear homogeneous group in the* $GF[p^n]$, $p > 2$, *defined by a quadratic invariant of determinant not zero, can be transformed by a linear homogeneous substitution belonging to the field into one of the two groups:*

1°. *The orthogonal group, with the invariant* $\sum_{i=1}^{m} \xi_i^2$.

---

*The theory of Galois is used in its abstract form, as presented by Moore in the Congress Mathematical Papers, 1893.

2°. *The group on an even number of indices with the invariant*
$$\sum_{i=1}^{m-1}\xi_i^2+\nu\xi_m^2\,.$$

2. Denote by $G_{m,\,p^n}^{(s)}$ the group leaving f_s invariant. The conditions that any substitution

$$S:\quad \xi_i'=\sum_{j=1}^{m}\alpha_{ij}\xi_j \qquad (i=1,\,2,\,\ldots.\,,\,m)$$

shall leave f_s invariant are as follows:*

$$(1).\quad \alpha_{1j}^2+\alpha_{2j}^2+\ldots.+\alpha_{sj}^2+\nu\,(\alpha_{s+1j}^2+\ldots.+\alpha_{mj}^2)=\begin{cases}1, & (j\overline{<}s)\\ \nu, & (j>s)\end{cases}$$

$$(2).\quad \alpha_{1j}\alpha_{1k}+\ldots.+\alpha_{sj}\alpha_{sk}+\nu\,(\alpha_{s+1j}\alpha_{s+1k}+\ldots.+\alpha_{mj}\alpha_{mk})=0.$$
$$(j,\,k=1,\,\ldots.\,,\,m\,;\;j\neq k)$$

It follows that the reciprocal of S is

$$S^{-1}:\begin{cases}\xi_i'=\displaystyle\sum_{j=1}^{m}\alpha_{ji}\xi_j+\nu\sum_{j=s+1}^{m}\alpha_{ji}\xi_j, & (i=1,\,\ldots.\,,\,s)\\[2ex] \xi_i'=\displaystyle\frac{1}{\nu}\sum_{j=1}^{s}\alpha_{ji}\xi_j+\sum_{j=s+1}^{m}\alpha_{ji}\xi_j. & (i=s+1,\,\ldots.\,,\,m)\end{cases}$$

The determinant of S^{-1} is seen to be equal to the determinant Δ of S. Hence $\Delta^2=1$, being the determinant of $S^{-1}S\equiv 1$. Writing the relations (1) and (2) for the substitution S^{-1}, we obtain the relations

$$(1').\quad \alpha_{j1}^2+\alpha_{j2}^2+\ldots.+\alpha_{js}^2+\frac{1}{\nu}\,(\alpha_{js+1}^2+\ldots.+\alpha_{jm}^2)=\begin{cases}1, & (j\overline{<}s)\\ 1/\nu, & (j>s)\end{cases}$$

$$(2').\quad \alpha_{j1}\alpha_{k1}+\ldots.+\alpha_{js}\alpha_{ks}+\frac{1}{\nu}\,(\alpha_{js+1}\alpha_{ks+1}+\ldots.+\alpha_{jm}\alpha_{km})=0.$$

$$(j,\,k=1,\,\ldots.\,,\,m\,;\;j\neq k)$$

These relations are together equivalent to the set (1), (2).

3. Lemma: *The number of systems of solutions* $\xi_1,\,\ldots.\,,\,\xi_{2m}$ *in the* $GF[p^n]$, $p>2$, *of the equation*

$$\alpha_1\xi_1^2+\alpha_2\xi_2^2+\ldots.+\alpha_{2m}\xi_{2m}^2=\varkappa,$$

---

* The conditions (2) do not occur if $p=2$, a case now excluded.

where every α_j *is a mark* $\neq 0$ *of the field, is*

$$p^{n(2m-1)} - \nu p^{n(m-1)}, \qquad (\varkappa \neq 0)$$
$$p^{n(2m-1)} + \nu (p^{nm} - p^{n(m-1)}), \qquad (\varkappa = 0)$$

where ν *is* $+1$ *or* -1 *according as* $(-1)^m \alpha_1\alpha_2 \ldots \alpha_{2m}$ *is a square or a not-square in the field. The number of solutions of*

$$\alpha_1\xi_1^2 + \alpha_2\xi_2^2 + \ldots + \alpha_{2m+1}\xi_{2m+1}^2 = \varkappa$$

is $p^{2nm} + \nu' p^{nm}$, *where* ν' *is* $+1$, -1 *or* 0 *according as* $(-1)^m\alpha_1\alpha_2 \ldots \alpha_{2m+1}\varkappa$ *is a square, not-square or zero in the* $GF[p^n]$.

These results follow from an immediate generalization of §§197–199, 201–212 of Jordan, "Traité des Substitutions," or of pp. 486–491 of Bachmann, Zahlentheorie, IV.

4. Lemma: *If* S *denote the number of squares* in the* $GF[p^n]$ *followed by squares and* N *the number of squares followed by not-squares, we have*

$$S = \tfrac{1}{4}(p^n - 5), \quad N = \tfrac{1}{4}(p^n - 1), \qquad \textit{if } -1 = \textit{square};$$
$$S = \tfrac{1}{4}(p^n - 3), \quad N = \tfrac{1}{4}(p^n + 1), \qquad \textit{if } -1 = \textit{not-square}.$$

Indeed, the number of sets of solutions ξ, η in the $GF[p^n]$ of the equation

$$\eta^2 = \xi^2 + 1$$

is always $p^n - 1$ (by §3). These solutions are of three kinds:

$$1^\circ. \quad \xi = 0 \quad , \quad \eta = \pm 1;$$
$$2^\circ. \quad \xi^2 = -1, \quad \eta = 0 \quad ,$$

occurring when -1 is a square;

$$3^\circ. \quad \xi^2 = \alpha \neq 0, \quad \eta^2 = \alpha + 1 \neq 0,$$

giving $4S$ sets of solutions ξ, η.

Hence, if -1 be a square, we have

$$p^n - 1 = 2 + 2 + 4S, \quad N + S + 1 = \tfrac{1}{2}(p^n - 1).$$

If -1 be a not-square, we have

$$p^n - 1 = 2 + 4S, \quad N + S = \tfrac{1}{2}(p^n - 1).$$

---

* The mark zero is not reckoned as a square.

5. Theorem: *The order of the group* $G^{(s)}_{m,\,p^n}$ *is, for m odd,*

$$2\,(p^{n(m-1)}-1)\,p^{n(m-2)}\,(p^{n(m-3)}-1)\,p^{n(m-4)}\,\ldots\ldots\,(p^{2n}-1)\,p^n,$$

*and, for m even,**

$$2\,[p^{n(m-1)}-(-1)^s\varepsilon^{\frac{m}{2}}p^{n\left(\frac{m}{2}-1\right)}](p^{n(m-2)}-1)\,p^{n(m-3)}\,\ldots\ldots\,(p^{2n}-1)\,p^n,$$

where $\varepsilon=\pm 1$ *according as* p^n *is of the form* $4l\pm 1$.

Let $N^{(s)}_m$ denote the number of substitutions $S, S', \ldots\ldots$ in the group which leave ξ_1 fixed. Let a general substitution T of the group replace ξ_1 by

$$F_1\equiv\sum_{j=1}^{m}\alpha_{1j}\xi_j, \quad \sum_{j=1}^{s}\alpha^2_{1j}+\frac{1}{\nu}\sum_{j=s+1}^{m}\alpha^2_{1j}=1.$$

The $N^{(s)}_m$ substitutions $TS, TS', \ldots\ldots$, and no others, will replace ξ_1 by F_1. If, therefore, $P^{(s)}_m$ denotes the number of distinct linear functions F_1 by which the substitutions of the group can replace ξ_1, we have for the order of the group,

$$\Omega^{(s)}_{m,\,p^n}=N^{(s)}_m P^{(s)}_m.$$

For the substitutions $S, S', \ldots\ldots$, we have

$$\alpha_{11}=1,\quad \alpha_{1j}=0. \qquad (j=2,\ldots\ldots,m)$$

Then by the relations (2′),

$$\alpha_{k1}=0. \qquad (k=2,3,\ldots\ldots,m)$$

The substitutions $S, S', \ldots\ldots$, therefore belong to the group $G^{(s-1)}_{m-1,\,p^n}$, leaving invariant

$$\sum_{i=2}^{s}\xi_i^2+\nu\sum_{i=s+1}^{m}\xi_i^2.$$

Hence

$$N^{(s)}_m=\Omega^{(s-1)}_{m-1,\,p^n}.$$

Repeating this argument, we find that

$$\Omega^{(s)}_{m,\,p^n}=P^{(s)}_m\Omega^{(s-1)}_{m-1,\,p^n}=P^{(s)}_m P^{(s-1)}_{m-1}\ldots\ldots P^{(2)}_{m-s+2}\Omega^{(1)}_{m-s+1,\,p^n},$$

where $\Omega^{(1)}_{m-s+1,\,p^n}$ is the order of the group leaving invariant ξ_m^2 or $\xi_{m-1}^2+\nu\xi_m^2$, according as $s=m$ or $s=m-1$, and therefore equals 2 or $2P^{(1)}_2$ respectively. Hence

$$\Omega^{(m)}_{m,\,p^n}=P^{(m)}_m\;P^{(m-1)}_{m-1}\ldots\ldots P^{(2)}_2\,.\,2,$$
$$\Omega^{(m-1)}_{m,\,p^n}=P^{(m-1)}_m P^{(m-2)}_{m-1}\ldots\ldots P^{(2)}_3 P^{(1)}_2\,.\,2.$$

---

* For $m=2$, the terms at the end of the formula do not occur.

It is proven in §§7–12 that the number $P_k^{(l)}$ is equal to the number of sets of solutions in the $GF[p^n]$ of the equation

$$\sum_{j=1}^{l} \alpha_j^2 + \frac{1}{\nu} \sum_{j=l+1}^{k} \alpha_j^2 = 1,$$

which, by §3, is seen to be as follows:

$$p^{n(k-1)} - (-1)^{k-l} \varepsilon^{\frac{k}{2}} p^{n\left(\frac{k}{2}-1\right)}, \qquad (k \text{ even})$$

$$p^{n(k-1)} + (-1)^{k-l} \varepsilon^{\frac{k-1}{2}} p^{n(k-1)/2}, \qquad (k \text{ odd})$$

ε denoting ± 1 according as -1 is a square or a not-square in the $GF[p^n]$. Whether t be even or odd, we have

$$P_{2t+1}^{(l)} \cdot P_{2t}^{(l-1)} = (p^{2nt} - 1) p^{n(2t-1)}.$$

We derive at once the expressions for the order $\Omega_{m,\,p^n}^{(s)}$ as given in the theorem.

6. Theorem: *The orthogonal group* $G_{m,\,p^n}^{(m)}$ *is generated by the substitutions [only the indices altered being written],*

$$C_i: \quad \xi_i' = -\xi_i,$$

$$O_{i,\,j}^{\alpha,\,\beta}: \quad \begin{cases} \xi_i' = \alpha\xi_i + \beta\xi_j, \\ \xi_j' = -\beta\xi_i + \alpha\xi_j, \end{cases} \qquad (\alpha^2 + \beta^2 = 1)$$

with the two following exceptions: *

for $p^n = 5$, $m \gtreqless 3$, *we may take as the necessary additional generator the substitution of period two,*

$$R: \begin{cases} \xi_1' = \xi_1 + \xi_2 + 2\xi_3, \\ \xi_2' = \xi_1 + 2\xi_2 + \xi_3, \\ \xi_3' = 2\xi_1 + \xi_2 + \xi_3; \end{cases}$$

for $p^n = 3$, $m \gtreqless 4$, *we may choose as the additional generator*

$$W: \begin{cases} \xi_1' = \xi_1 - \xi_2 - \xi_3 - \xi_4, \\ \xi_2' = \xi_1 - \xi_2 + \xi_3 + \xi_4, \\ \xi_3' = \xi_1 + \xi_2 - \xi_3 + \xi_4, \\ \xi_4' = \xi_1 + \xi_2 + \xi_3 - \xi_4. \end{cases} \qquad (W^3 = 1)$$

* These exceptions were overlooked by Jordan in his treatment of the case $n = 1$.

The group $G_{m,\,p^n}^{(m-1)}$ *is generated by the substitutions* C_i, $O_{i,\,j}^{\alpha,\,\beta}$ $(i, j < m)$ *together with*

$$O_{i,\,m}^{\gamma,\,\delta}:\ \begin{cases} \xi_i' = \gamma\xi_i + \delta\xi_m\,, \\ \xi_m' = -\dfrac{\delta}{\nu}\,\xi_i + \gamma\xi_m, \end{cases} \qquad \left(\gamma^2 + \frac{1}{\nu}\delta^2 = 1\right)$$

an additional generator being necessary if $p^n = 3$, $m \geqq 3$, *viz.*

$$V_{1,\,2,\,m}:\ \begin{cases} \xi_1' = \xi_1 - \xi_2 - \xi_m, \\ \xi_2' = \xi_1 - \xi_2 + \xi_m, \\ \xi_m' = -\xi_1 - \xi_2 \end{cases} \qquad (V^3 = 1)$$

Our theorem is evident if $m = 2$. For $m \geqq 3$, it will follow from §5 by applying the results of §§7–12.

7. Theorem: *If* $\alpha_1, \alpha_2, \alpha_3$ *be any set of solutions in the* $GF[p^n]$ *of the equation*

$$\alpha_1^2 + \alpha_2^2 + \frac{1}{\mu}\alpha_3^2 = 1$$

(where $\mu = 1$ *or the not-square* ν*), there exists a substitution* S *derived from the generators of* §6 *which leave invariant*

$$\xi_1^2 + \xi_2^2 + \mu\xi_3^2,$$

such that S *will replace* ξ_1 *by* $\alpha_1\xi_1 + \alpha_2\xi_2 + \alpha_3\xi_3$.

The proposition follows at once if $1 - \alpha_1^2$ or $1 - \alpha_2^2$ be a square (excluding zero) in the $GF[p^n]$. For, if $1 - \alpha_2^2 = \tau^2$, then

$$\frac{\alpha_1^2}{\tau^2} + \frac{1}{\mu}\,\frac{\alpha_3^2}{\tau^2} = 1.$$

We may therefore take

$$S = (\xi_1\xi_2)\, O_{2,\,3}^{\frac{\alpha_1}{\tau},\,-\frac{\alpha_3}{\tau}}\, O_{1,\,2}^{\alpha_2,\,\tau}.$$

The proposition is true for the quantities $\alpha_1, \alpha_2, \alpha_3$ *if true for*

$$\alpha_1' \equiv \alpha_1, \quad \alpha_2' \equiv \beta\alpha_2 + \frac{\gamma}{\mu}\alpha_3, \quad \alpha_3' \equiv -\gamma\alpha_2 + \beta\alpha_3,$$

where

$$\beta^2 + \frac{1}{\mu}\gamma^2 = 1.$$

We notice that

$$\alpha_1'^2 + \alpha_2'^2 + \frac{1}{\mu}\alpha_3'^2 = \alpha_1^2 + \alpha_2^2 + \frac{1}{\mu}\alpha_3^2 = 1. \tag{3}$$

Then, if the group contains a substitution S' replacing ξ_1 by $\alpha_1'\xi_1 + \alpha_2'\xi_2 + \alpha_3'\xi_3$, it will contain the product $O_{2,3}^{\beta,\gamma} S'$ which replaces ξ_1 by $\alpha_1\xi_1 + \alpha_2\xi_2 + \alpha_3\xi_3$.

Similarly, the proposition is true for α_1, α_2, α_3 if true for the quantities

$$\alpha_1' \equiv \alpha_1\rho - \alpha_2\sigma, \quad \alpha_2' \equiv \alpha_1\sigma + \alpha_2\rho, \quad \alpha_3' \equiv \alpha_3,$$

where

$$\rho^2 + \sigma^2 = 1.$$

8. Consider first the case in which -1 is a not-square in the $GF[p^n]$. There are (by §3) $p^n + 1$ sets of solutions ρ, σ in the field of the equation $\rho^2 + \sigma^2 = 1$. Not more than two of these sets of solutions give the same value to

$$\alpha_2' \equiv \alpha_1\sigma + \alpha_2\rho.$$

Indeed, by eliminating σ, we obtain a quadratic for ρ. Hence α_2' takes at least $\frac{1}{2}(p^n + 1)$ distinct values. But by §4 there are exactly $\frac{1}{2}(p^n - 3)$ distinct marks $\eta \neq 0$ for which $\eta^2 - 1$ is a square, i. e. for which $1 - \eta^2$ is a not-square. Hence there exist at least two values of α_2' for which $1 - \alpha_2'^2$ is a square or zero. If it be a square, our theorem follows from the remark at the end of the last paragraph.

It remains to consider the case $\alpha_2'^2 = 1$. Then by (3),

$$\alpha_1'^2 = -\frac{1}{\mu}\alpha_3'^2.$$

If $\mu = 1$, we have $\alpha_1' = \alpha_3' = 0$ and the theorem is evident. If μ be a not-square, we may take $\mu = -1$. Then

$$\alpha_1' = \pm\alpha_3', \quad \alpha_2'^2 = 1.$$

As in §7, the theorem is true for α_1', α_2', α_3' if true for the quantities

$$\alpha_1'' \equiv \alpha_1'\beta - \alpha_3'\gamma, \quad \alpha_2'' \equiv \alpha_2', \quad \alpha_3'' \equiv -\gamma\alpha_2' + \beta\alpha_3',$$

where

$$\beta^2 - \gamma^2 = 1.$$

The $p^n - 1$ solutions of this equation are given by

$$\beta = \tfrac{1}{2}\left(\tau + \frac{1}{\tau}\right), \quad \mp\gamma = \tfrac{1}{2}\left(\tau - \frac{1}{\tau}\right),$$

where τ runs through the marks $\neq 0$ of the $GF[p^n]$. Hence $\beta \mp \gamma$ may be given an arbitrary value $\tau \neq 0$ in the field. The theorem being evident if $\alpha_1' = 0$, we exclude this case. Then $\alpha_1'' \equiv \alpha_1' (\beta \mp \gamma)$ may be made to assume an arbitrary value except zero, and hence, if $p^n > 3$, a value for which $1 - \alpha_1''^2$ is a square in the field.

It remains to consider, when $p^n = 3$, the case in which

$$\alpha_1' = \pm \alpha_3' \neq 0, \quad \alpha_2'^2 = 1, \quad \mu = -1.$$

Since α_1', α_2', α_3' are each ± 1, we may evidently take

$$S = CV,$$

where C is a product formed from C_1, C_2, C_3.

9. Suppose next that -1 is the square of a mark I belonging to the $GF[p^n]$. If μ be a not-square, there exist $p^n + 1$ sets of solutions in the field of the equation

$$\beta^2 + \frac{1}{\mu}\gamma^2 = 1. \tag{4}$$

By §7, the theorem is true if proven true for the values

$$\alpha_1' \equiv \alpha_1, \quad \alpha_2' \equiv \beta\alpha_2 + \frac{\gamma}{\mu}\alpha_3, \quad \alpha_3' \equiv -\gamma\alpha_2 + \beta\alpha_3.$$

There are at least $\frac{1}{2}(p^n + 1)$ sets of solutions of (4) for which the values of α_2' are distinct; for upon eliminating β we obtain a quadratic for γ. But by §4 there exist only $\frac{1}{2}(p^n - 1)$ marks $I\xi$, and hence as many distinct values of ξ, for which $(I\xi)^2 + 1 \equiv 1 - \xi^2$ is a not-square. Hence at least one set of solutions of (4) will make $1 - \alpha_2'^2$ a square or zero. If it be a square, the theorem follows from §7. If it be zero, (3) gives

$$\alpha_1'^2 = -\frac{1}{\mu}\alpha_3'^2.$$

Since μ is a not-square and -1 a square, we have

$$\alpha_1' = \alpha_3' = 0, \quad \alpha_2'^2 = 1,$$

so that we may take as the required substitution

$$\xi_1' = \alpha_2' \xi_2, \quad \xi_2' = \xi_1, \quad \xi_3' = \xi_3.$$

10. There remains the case in which -1 and μ are both squares. We may take $\mu = 1$, so that we have

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1.$$

There are now $p^n - 1$ sets of solutions of (4). These give at least $\frac{1}{2}(p^n - 1)$ distinct values of α_2'. Hence α_2' must take a value for which $1 - \alpha_2'^2$ is a square or zero or else be capable of taking *every* value for which $1 - \alpha_2'^2$ is a not-square. If it be a square, the theorem follows at once. If it be zero, we have

$$\alpha_2'^2 = 1, \quad \alpha_1'^2 + \alpha_3'^2 = 0. \tag{5}$$

If $\alpha_3' = 0$, the proposition follows at once. Suppose that $\alpha_3' \neq 0$. The proposition will be true for α_1', α_2', α_3' if proven for

$$\alpha_1'' \equiv \alpha_1' \rho - \alpha_3' \sigma, \quad \alpha_2'' \equiv \alpha_2' \quad \alpha_3'' \equiv \alpha_1' \sigma + \alpha_3' \rho,$$

where

$$\rho^2 + \sigma^2 = 1.$$

We can give to α_1'' an arbitrary value $\neq 0$ in the $GF[p^n]$. Indeed, on eliminating σ, we obtain for ρ the *linear* equation (the coefficient of ρ^2 being zero),

$$\rho^2 \left(1 + \frac{\alpha_1'^2}{\alpha_3'^2}\right) - 2 \frac{\alpha_1'' \alpha_1'}{\alpha_3'^2} \rho + \left(\frac{\alpha_1''}{\alpha_3'}\right)^2 = 1.$$

But by §4 there are $\frac{1}{4}(p^n - 5)$ squares τ^2 for which $\tau^2 - 1$ and hence also $1 - \tau^2$ is a square. Our theorem therefore follows if $p^n \neq 5$.

There remains the case in which α_2' may take every one of the values for which $1 - \alpha_2'^2$ is a not-square. Repeating the same arguments for the quantities α_1'', α_2'' α_3'', we find that, for $p^n \neq 5$, the only case in which the theorem is not proven is that in which α_1'' and α_2'' may each take every one of the $\frac{1}{2}(p^n - 1)$

values δ for which $1-\delta^2$ is a not-square. Hence if our theorem be true for one such set of quantities

$$\alpha_1'' = \delta_1, \quad \alpha_2'' = \delta_2, \quad \alpha_3'',$$

it is true for every set; if false for one, it is false for every set. Further, we have

$$\alpha_1''^2 + \alpha_2''^2 + \alpha_3''^2 = \alpha_1'^2 + \alpha_2'^2 + \alpha_3'^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1 .$$

Hence, whatever one of the $\{\frac{1}{2}(p^n-1)\}^2$ pairs of values we take for δ_1, δ_2, we can satisfy the equation

$$\delta_1^2 + \delta_2^2 + \delta_3^2 = 1$$

in two ways, viz. by $\delta_3 = \pm \alpha_3''$. This equation has therefore $\frac{1}{2}(p^n-1)^2$ sets of solutions δ_1, δ_2, δ_3 for which $1-\delta_1^2$ and $1-\delta_2^2$ are not-squares. By virtue of the substitution C_3, the proposition is true for $\delta_1, \delta_2, -\delta_3$ if it be true for $\delta_1, \delta_2, +\delta_3$. If therefore our theorem be not always true, it will be false for all of the above $\frac{1}{2}(p^n-1)^2$ sets of values. It has been proven true for all other sets of solutions of

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = 1 .$$

The total number of sets of solutions is (by §3) $p^{2n} + p^n$, -1 being a square.

The substitutions of the ternary orthogonal group would therefore replace ξ_1 by

$$R_3 \equiv p^{2n} + p^n - \tfrac{1}{2}(p^n-1)^2 = \tfrac{1}{2}(p^{2n} + 4p^n - 1)$$

distinct linear functions. The number of substitutions leaving ξ_1 fixed is clearly $2(p^n-1)$. The order of the group would thus be

$$(p^{2n} + 4p^n - 1)(p^n - 1) .$$

This number must divide the order of the general ternary linear homogeneous group in the $GF[p^n]$, viz.

$$(p^{3n}-1)(p^{3n}-p^n)(p^{3n}-p^{2n}) .$$

Hence $p^{2n} + 4p^n - 1$, which is relatively prime to p, must divide $(p^{3n}-1)(p^{2n}-1)$ and hence also

$$4p^n(p^{3n}-1) \equiv 4p^n\{(p^n-4)(p^{2n}+4p^n-1) + 17p^n - 5\} .$$

It must therefore divide $4(17p^n - 5)$ and hence also

$$20(p^{2n} + 4p^n - 1) - (68p^n - 20) = p^n(20p^n + 12).$$

Hence $(p^n + 2)^2 - 5$ must divide 304; indeed

$$3(68p^n - 20) + 5(20p^n + 12) = 304p^n.$$

Hence $$p^n + 2 < 18 > \sqrt{309}.$$

But the only values of $p^n < 16$ for which -1 is a square in the $GF[p^n]$ are $p^n = 13, 9, 5$. For none of these is $(p^n + 2)^2 - 5$ a divisor of $304 \equiv 16.19$.

11. There remains the case $p^n = 5$, $\mu = 1$, not treated in §10 in the two following sub-cases:

For the case in which (5) holds, we have

$$\alpha_2'^2 = 1, \quad \alpha_1'^2 = \pm 1, \quad \alpha_3'^2 = \mp 1,$$

the only squares being ± 1. We may therefore take $S = TR$, T being derived from C_1, C_2, C_3 and $(\xi_1 \xi_3)$.

For the case in which $1 - \alpha_2'^2$ is a not-square, we have

$$\alpha_2'^2 = -1, \quad \alpha_1'^2 = 1, \quad \alpha_3'^2 = 1.$$

Then will $S = C(\xi_2 \xi_3) R$, where C is derived from C_1, C_2, C_3, replace ξ_1 by $\alpha_1' \xi_1 + \alpha_2' \xi_2 + \alpha_3' \xi_3$.

Note: R cannot be derived from the C_i and $O_{i,j}^{\alpha,\beta}$; indeed, the latter are of the form $C_i C_j$, or the identity, or

$$\xi_i' = \pm \xi_j, \quad \xi_j' = \mp \xi_i.$$

12. Theorem: *If* $\alpha_1, \alpha_2, \ldots, \alpha_m$ *be any set of solutions in the* $GF[p^n]$ *of*

$$\alpha_1^2 + \alpha_2^2 + \ldots + \alpha_{m-1}^2 + \frac{1}{\mu}\alpha_m^2 = 1,$$

there exists a substitution S *derived from the generators of* §6 *which leave invariant* $\sum_{i=1}^{m-1} \xi_i^2 + \mu \xi_m^2$ *such that* S *will replace* ξ_1 *by* $\sum_{j=1}^{m} \alpha_j \xi_j$.

The proposition being true for $m = 2$ and $m = 3$, we will make a proof by induction from $m - 1$ to m, supposing $m > 3$.

Consider first the cases in which every sum of three of the terms $\alpha_1^2, \alpha_2^2, \ldots, \alpha_{m-1}^2, \frac{1}{\mu}\alpha_m^2$ is zero. These terms must all be equal and therefore

$$m\alpha_1^2 = 1, \quad 3\alpha_1^2 = 0, \quad \mu = \text{square}.$$

Hence $p = 3$, while m is of the form $3k + 2$ or $3k + 1$.

If $m = 3k + 2$, we have $1 - \alpha_1^2 = \alpha_1^2 \neq 0$, so that the theorem is reduced by §7 to the case of $m - 1$ indices.

If $m = 3k + 1$, we must have $\alpha_1^2 = 1$. But the product $O_{1,2}^{\alpha,\beta} S$ will replace ξ_1 by $\alpha_1'\xi_1 + \ldots + \alpha_m'\xi_m$, where

$$\alpha_1' \equiv \alpha\alpha_1 - \beta\alpha_2, \quad \alpha_2' \equiv \beta\alpha_1 + \alpha\alpha_2, \quad \alpha_j' \equiv \alpha_j. \qquad (j = 3, \ldots, m)$$

Of the $3^n \pm 1$ sets of values in the $GF[3^n]$ satisfying

$$\alpha^2 + \beta^2 = 1,$$

at most two give the same value to α_1' and hence at most four make $\alpha_1'^2 = 1$. Hence, if $n > 1$, we can avoid the case $\alpha_1^2 = 1$. For $p^n = 3$, we may take

$$S = C W_{1234} W_{1567} \ldots W_{1\,3k-1\,3k\,3k+1},$$

where C is derived from the C_i and W is defined in §6. There remains for consideration the case in which, for example,*

$$\alpha_1^2 + \alpha_2^2 + \frac{1}{\mu}\alpha_m^2 \neq 0.$$

The treatment for a case like $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$ is quite similar, taking $\mu = 1$.

We have proven that, for every set of solutions of

$$\alpha^2 + \beta^2 + \frac{1}{\mu}\gamma^2 = 1, \tag{6}$$

there exists a substitution Σ of the group

$$\xi_1' = \alpha\xi_1 + \beta\xi_2 + \gamma\xi_m, \quad \xi_2' = \alpha'\xi_1 + \beta'\xi_2 + \gamma'\xi_m, \quad \xi_m' = \alpha''\xi_1 + \beta''\xi_2 + \gamma''\xi_m,$$

---

*For the case $p^n = 5$, $m \overset{=}{>} 4$, $\mu =$ not-square, it would appear that the generator R were necessary in addition to the C_i and $O_{i,j}^{\alpha,\beta}$. We can, however, express R in terms of the generators

$$O_{i,m}^{2,1}: \begin{cases} \xi_i' = 2\xi_i + \xi_m \\ \xi' = 3\xi_i + 2\xi_m \end{cases},$$

leaving invariant $\xi_1^2 + \xi_2^2 + \ldots + \xi_{m-1}^2 + 3\xi_m^2$. Indeed,

$$R = O_{1m} O_{2m} O_{3m}^{-1} O_{1m} O_{2m}^{-1} O_{3m}^{-1}.$$

which therefore satisfies the relation (6) and the following:

$$\alpha'^2 + \beta'^2 + \frac{1}{\mu}\gamma'^2 = 1, \quad \alpha^2 + \alpha'^2 + \mu\alpha''^2 = 1, \quad \alpha\beta + \alpha'\beta' + \mu\alpha''\beta'' = 0, \text{ etc.}$$

If there be a substitution S' in our group which replaces ξ_1 by

$$\alpha_1'\xi_1 + \alpha_2'\xi_2 + \alpha_m'\xi_m + \sum_{j=3}^{m-1} \alpha_j\xi_j,$$

where

$$\alpha_1' = \alpha\alpha_1 + \beta\alpha_2 + \frac{\gamma}{\mu}\alpha_m,$$
$$\alpha_2' = \alpha'\alpha_1 + \beta'\alpha_2 + \frac{\gamma'}{\mu}\alpha_m,$$
$$\alpha_m' = \mu\alpha''\alpha_1 + \mu\beta''\alpha_2 + \gamma''\alpha_m,$$

then the group will contain $\Sigma S'$ which replaces ξ_1 by

$$\sum_{j=1}^{m} \alpha_j\xi_j.$$

The proposition is therefore true for the quantities α_j if true for α_1', α_2', α_m' $\alpha_4, \alpha_5, \ldots, \alpha_{m-1}$. We may thus make our proof by induction from $m-1$ to m by showing that it is possible to choose α, β, γ among the sets of solutions of (6) in such a way that $\alpha_1' = 0$. We may suppose that $\alpha_1 \neq 0$, since otherwise the proposition is already proven.

If $\alpha_1^2 + \alpha_2^2 = 0$, then $\alpha_2 \neq 0$. From $\frac{1}{\mu}\alpha_m^2 = 1$, it follows that μ is a square, say $\mu = 1$. Then the values

$$\alpha = \frac{-\alpha_m}{2\alpha_1}, \quad \beta = \frac{-\alpha_m}{2\alpha_2}, \quad \gamma = 1$$

satisfy (6) and make $\alpha_1' = 0$.

If $\alpha_1^2 + \alpha_2^2 \neq 0$, the condition (6) combines with $\alpha_1' = 0$ to give a single condition for β and γ:

$$\left(\beta\alpha_2 + \frac{\gamma}{\mu}\alpha_m\right)^2 + \alpha_1^2\left(\beta^2 + \frac{1}{\mu}\gamma^2\right) = \alpha_1^2.$$

Multiplying this by $\alpha_1^2 + \alpha_2^2$, it may be given the form

$$\left\{\beta(\alpha_1^2 + \alpha_2^2) + \frac{\alpha_2\alpha_m}{\mu}\gamma\right\}^2 + \frac{\gamma^2\alpha_1^2}{\mu}\left(\alpha_1^2 + \alpha_2^2 + \frac{\alpha_m^2}{\mu}\right) = \alpha_1^2(\alpha_1^2 + \alpha_2^2).$$

Since the coefficient of γ^2 is not zero, this equation has (by §3) $p^n \pm 1$ sets of solutions β, γ in the $GF[p^n]$.

13. *Note:* For the case $p^n = 3$, $m \gtreqless 4$, $\mu = -1$, it is readily seen that, instead of the additional generator V, we may take the more symmetrical substitution of period six:

$$X: \begin{cases} \xi_i' = \quad\; \xi_j + \xi_k + \xi_m, \\ \xi_j' = \xi_i \quad\; + \xi_k + \xi_m, \\ \xi_k' = \xi_i + \xi_j + \quad\; \xi_m, \\ \xi_m' = \xi_i + \xi_j + \xi_k - \xi_m, \end{cases}$$

where $(XC_1C_2C_3)^2 = 1$, $X^3 = C_1C_2C_3C_4$.

Structure of the Group $G_{m,\,p^n}^{(s)}$, §§14–32.

14. The substitutions of $G_{m,\,p^n}^{(s)}$ of determinant unity form a subgroup G of index 2. It is extended by C_1 to the total group.

By §3, there are $p^n - \varepsilon$ solutions α, β in the $GF[p^n]$ of

$$\alpha^2 + \frac{1}{\mu}\beta^2 = 1,$$

where $\varepsilon = +1$ or -1 according as $-\dfrac{1}{\mu}$ is a square or a not-square in the field. Hence the substitutions $O_{i,j}^{\alpha,\beta}$ which leave $\xi_i^2 + \mu\xi_j^2$ invariant and have the determinant unity form a group O_{ij} of order $p^n - \varepsilon$. Moreover, its substitutions are commutative; indeed

$$O_{i,j}^{\alpha',\beta'}O_{i,j}^{\alpha,\beta}: \begin{cases} \xi_i' = \quad\;\; \left(\alpha\alpha' - \dfrac{\beta\beta'}{\mu}\right)\xi_i + (\alpha\beta' + \alpha'\beta)\,\xi_j, \\ \xi_j' = -\left(\dfrac{\alpha\beta' + \alpha'\beta}{\mu}\right)\xi_i + \left(\alpha\alpha' - \dfrac{\beta\beta'}{\mu}\right)\xi_j \end{cases}$$

is unaltered if we interchange α with α', β with β'. We shall use a notation for the square of such a substitution,

$$Q_{i,j}^{\alpha,\beta} \equiv (O_{i,j}^{\alpha,\beta})^2: \begin{cases} \xi_i' = \quad (2\alpha^2 - 1)\,\xi_i + 2\alpha\beta\xi_j, \\ \xi_j' = -2\dfrac{\alpha\beta}{\mu}\xi_i + (2\alpha^2 - 1)\,\xi_j. \end{cases}$$

The substitutions $Q_{i,j}^{\alpha,\beta}$ form a commutative group Q_{ij} of order $\frac{1}{2}(p^n - \varepsilon)$. Indeed, we can have

$$Q_{i,j}^{\alpha,\beta} = Q_{i,j}^{\alpha',\beta'}$$

if and only if $\alpha' = \pm\alpha$, $\beta' = \pm\beta$.

For our group G we are concerned with the $O_{i,j}^{\alpha,\beta}$ in which $\mu = 1$, $\alpha^2 + \beta^2 = 1$ if $i, j < m$ or if $i < j = m = s$, or in which $\mu = \nu$, a not-square, $\alpha^2 + \frac{1}{\nu}\beta^2 = 1$, if $j = m = s + 1$. The product $C_i C_j$ is always of the form $O_{i,j}^{\alpha,\beta}$; it belongs to Q_{ij} if i, $j < m$, while $C_i C_m$ belongs to Q_{im} only when $s = m$.

If T_{ij} denote the transposition $(\xi_i \xi_j)$, $T_{ij} C_i$ belongs to O_{ij} if i, $j < m$ or $i < j = m = s$, but not to O_{im} if $s = m - 1$. Further, it belongs to Q_{ij}, when $m = s$, if and only if 2 is a square in the field.

15. Let ρ, σ be a set of solutions of $\rho^2 + \sigma^2 = 1$ such that $O_{1,2}^{\rho,\sigma}$ does not belong to the group $Q_{1,2}$. The substitution

$$M_{ij} \equiv O_{i,j}^{\rho,\sigma} \qquad (i, j < m)$$

serves to extend the group Q_{ij} to the group O_{ij}.

Similarly, for $s = m - 1$, if $\varkappa$, τ be a set of solutions of $\varkappa^2 + \frac{1}{\nu}\tau^2 = 1$ such that $O_{1,m}^{\varkappa,\tau}$ does not belong to Q_{1m}, the substitution

$$M_{im} \equiv O_{i,m}^{\varkappa,\tau} \qquad (i < m)$$

serves to extend the group Q_{im} to O_{im}. For example, we may take $M_{im} = C_i C_m$, ν being a not-square.

16. *For $p^n > 5$, or for $p^n = 5$ when $s = m - 1$, the group generated as follows:*

$$H \equiv \{ Q_{i,j}^{\alpha,\beta}, \quad M_{ij} M_{kl}, \quad (i, j, k, l = 1, 2, \ldots, m) \},$$

where α, β take all the values in the $GF[p^n]$ for which

$$\alpha^2 + \beta^2 = 1, \qquad (i, j < m;\ i < j = m \text{ if } s = m)$$

$$\alpha^2 + \frac{1}{\nu}\beta^2 = 1 \qquad (i < j = m, \text{ if } s = m - 1)$$

contains half of the substitutions of G.

Indeed, every substitution S of G has the form

$$S \equiv h_1 M_{ij} h_2 M_{kl} h_3 \ldots,$$

where the h_i belong to H. Further, M_{ij} is commutative with every $Q_{i,\,j}^{\alpha,\,\beta}$, $Q_{k,\,l}^{\alpha,\,\beta}$ $(k,\, l \neq i,\, j)$. Also

$$M_{ij}\, Q_{i,\,k}^{\alpha,\,\beta} \equiv M_{ij}\,(O_{i,\,k}^{\lambda,\,\mu})^2\, Q_{ik}^{\lambda,\,-\mu} \cdot Q_{i,\,k}^{\alpha,\,\beta}$$
$$= (M_{ij}\, O_{i,\,k}^{\lambda,\,\mu})(Q_{i,\,k}^{\lambda,\,-\mu}\, Q_{i,\,k}^{\alpha,\,\beta})\, Q_{i,\,k}^{\lambda,\,\mu} = h' M_{ik}$$

(where h' belongs to H), provided we take $\lambda,\, \mu = \rho,\, \sigma$ when $i,\, k < m$ or $i < k = m = s$, but take $\lambda,\, \mu = \varkappa,\, \tau$ when $i < k = m = s + 1$. Hence S takes the form h'' or else $h'' M_{r,\,s}$, where h'' belongs to H. If $s \gtrless 2$, we have the identity

$$M_{rs} = M_{rs}\, M_{21}\, M_{12} = h_1\, M_{12}.$$

Hence every substitution of G may be given one of the two forms, h or hM_{12}, where h belongs to H.

From the cases investigated (see §§30 and 49–55), it appears that H is not identical with G and hence of index two under it.

17. For $p^n = 5$, $m = s \overline{\gtrless} 3$, the group

$$H \equiv \{ C_i C_j, \quad T_{ij}\, T_{ik}, \quad (i,\, j,\, k = 1, \ldots\ldots, m), \quad R \}$$

is of index two under G. Indeed, 2 being a not-square modulo 5, $T_{12} C_1$ is not in the group Q_{12}. We readily see that $T_{12} C_1$ is commutative with the group H; for example, it transforms R into $C_2 C_3 R\, T_{12}\, T_{13}\, C_2 C_3$.

For $p^n = 3$, $m = s > 3$, the group

$$H \equiv \{ C_i C_j, \quad T_{ij}\, T_{ik}, \quad (i,\, j,\, k = 1, \ldots\ldots, m), \quad W \}$$

is of index two under G. Here also $T_{12} C_1$ is not in the group Q_{12} and is commutative with H; for example, it transforms W into $W^2 C_1 C_2$.

For $p^n = 3$, $m = s = 3$, the group of order twelve

$$H \equiv [1, \ C_i C_j \text{ (three)}, \quad T_{ij}\, T_{ik} \text{ (two)}, \quad T_{ij}\, T_{ik} C_r C_s \text{ (six)}]$$

is extended by $T_{12} C_1$ to the group G of order 24.

For $p^n = 3$, $m = 3$, $s = 2$, the group leaving $\xi_1^2 + \xi_2^2 - \xi_3^2$ invariant is obtained from that leaving $\xi_1^2 + \xi_2^2 + \xi_3^2$ by transforming by the substitution

$$O: \quad \xi_1' = \xi_1 - \xi_2, \quad \xi_2' = \xi_1 + \xi_2.$$

We find that O transforms $C_1 C_2$, $C_1 C_3$, $C_2 C_3$, $T_{12}\, T_{23}$, $T_{13}\, T_{23}$ into respectively

C_1C_2, $T_{12}C_1C_2C_3$, $T_{12}C_3$, V and $V^2 \equiv V^{-1}$. Hence O transforms the group H of the last paragraph into

$$H \equiv [V^i, \quad V^iC_1C_2, \quad V^iT_{12}C_3, \quad V^iT_{12}C_1C_2C_3]. \qquad (i=0,\ 1,\ 2)$$

For $p^n = 3$, $m > 3$, $s = m - 1$, the group generated as follows:

$$H \equiv \{C_iC_j, \quad T_{ij}C_m, \quad (i, j = 1, \ldots, m-1), \quad V_{1,2,m}\}$$

is of index two under G and is extended to G by the substitution $T_{12}C_1$. The latter transforms $V_{1,2,m}$ into

$$V^2_{1,2,m}C_1C_2.$$

18. Theorem: *When G is the orthogonal group (viz. $s = m$), the squares of its substitutions generate the group H.* Indeed, the squares of

$$O^{\alpha,\beta}_{1,2}, \quad O^{\alpha,\beta}_{1,2}T_{13}C_1C_2C_3, \quad O^{\alpha,\beta}_{1,2}T_{13}T_{24}$$

are respectively

$$Q^{\alpha,\beta}_{1,2}, \quad O^{\alpha,\beta}_{1,2}O^{\alpha,\beta}_{3,2}, \quad O^{\alpha,\beta}_{1,2}O^{\alpha,\beta}_{3,4}.$$

For $p^n > 5$, H is generated by substitutions of these three types.

For $p^n = 5$ or 3, we have respectively

$$(RC_1C_2)^2 = T_{12}T_{23}C_1C_2RC_1C_3, \quad W^2 = W^{-1},$$

so that we obtain the necessary additional generators R or W respectively.

19. Every linear homogeneous substitution on m indices is commutative with

$$C \equiv C_1C_2 \ldots C_m: \quad \xi_i' = -\xi_i, \qquad (i = 1, \ldots, m)$$

of determinant $(-1)^m$. If m be odd, C does not belong to H. If m be even and $s = m$, C belongs to H. If m be even and $s = m - 1$, it seems probable that C does not belong to H, since it serves to extend H to G [see §§49–53 for the cases $m = 6$ and $m = 4$].

Suppose that H has an invariant subgroup I containing a substitution

$$S: \quad \xi_i' = \sum_{j=1}^{m} \alpha_{ij}\xi_j, \qquad (i = 1, \ldots, m)$$

neither the identity nor C. We will prove that I coincides with H when m is odd, the case $p^n = 3$, $m = 3$ being an exception, and when m is even and > 2, the case $m = 4$, $s = 4$ being an exception. The method of proof consists in deriving from S and its transformed by substitutions in H a substitution belonging to I and affecting at most three indices. Then I will contain all such substitutions, since the subgroup of H affecting only three indices is simple, aside from the case $p^n = 3$. It then follows that I coincides with H.

20. If the above substitution S be of the form

$$\xi_i' = \alpha_{ii}\xi_i, \qquad (i = 1 \ldots\ldots m) \tag{7}$$

where therefore $\alpha_{ii}^2 = 1$, it is merely a product of an even number of the C_i's, in which certain ones as C_k are lacking, since S is neither the identity nor $C_1 C_2 \ldots\ldots C_m$. But if $S = C_i C_j C_r C_s \ldots\ldots$, its transformed by $T_{ij}\, T_{ik}$, belonging to H, gives $S' = C_k C_j C_r C_s \ldots\ldots$ Hence I contains

$$S' S^{-1} = C_k C_i .$$

If S is not of the form (7), we may assume that $\alpha_{12}, \alpha_{13}, \ldots\ldots, \alpha_{1m}$ are not all zero. For either S or its reciprocal will have at least one α_{ij} $(i < j)$ different from zero. Transforming by $T_{1j}\, T_{1i}$, we have a substitution in I replacing ξ_1 by

$$\alpha_{ii}\xi_1 + \alpha_{ij}\xi_i + \ldots\ldots$$

21. Theorem: *If $m > 4$, the group I contains a substitution not the identity in which $\alpha_{12} = 0$.*

We denote by μ a not-square ν when $s = m - 1$ and the square unity when $s = m$. If $\alpha_{12} \neq 0$, we transform* S by

$$O_{234m} \left\{ \begin{array}{l} \xi_2' = \alpha\xi_2 + \beta\xi_3 + \gamma\xi_4 + \delta\xi_m, \\ \xi_3' = \alpha'\xi_2 + \beta'\xi_3 + \gamma'\xi_4 + \delta'\xi_4, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{array} \right.$$

$$\left(\alpha^2 + \beta^2 + \gamma^2 + \frac{1}{\mu}\,\delta^2 = 1, \text{ etc.}\right)$$

---

*If O_{234m} does not belong to H, its product by O_{4m} will belong to H, O_{4m} being suitably chosen. A similar remark is understood to apply in the succeeding paragraphs.

The coefficients in the resulting substitution are

$$\alpha'_{11} = \alpha_{11}, \quad \alpha'_{12} = \alpha\alpha_{12} + \beta\alpha_{13} + \gamma\alpha_{14} + \frac{\delta}{\mu}\alpha_{1m}, \text{ etc.}$$

As in §12, we can determine $\alpha, \beta, \gamma, \delta$ so that $\alpha'_{12} = 0$, unless perhaps in the case for which

$$p = 3, \quad \mu = 1, \quad \alpha^2_{12} = \alpha^2_{13} = \alpha^2_{14} = \alpha^2_{1m}.$$

In this case the transformed of S by KW_{324m}, K being a suitable product formed from C_2, C_3, C_4, C_m, will give a substitution belonging to I in which $\alpha'_{12} = \alpha'_{14} = \alpha'_{1m} = 0$.

22. Theorem: *If $m > 4$, the group I contains a substitution affecting only two indices or else a substitution in which α_{12} has an arbitrary value τ in the $GF[p^n]$.*

In virtue of §20, it remains to consider the case in which not every α_{1j} $(j = 2, \ldots, m)$ is zero.

If $\alpha_{1m} \neq 0$, $\alpha_{1j} = 0$ $(j = 2, \ldots, m-1)$, we transform S by $O^{\alpha, \beta, \gamma}_{2, 3, m}$, obtaining a substitution S' in which

$$\alpha'_{12} = \alpha\alpha_{12} + \beta\alpha_{13} + \frac{\gamma}{\mu}\alpha_{1m}.$$

Taking $\gamma = \dfrac{\mu\tau}{\alpha_{1m}}$ and α, β such that $\alpha^2 + \beta^2 + \dfrac{\gamma^2}{\mu} = 1$, we have in S' a substitution belonging to I and having $\alpha'_{12} = \tau$.

If $\alpha_{12}, \alpha_{13}, \ldots, \alpha_{1m-1}$ are not all zero, we may make $\alpha_{12} = 0$ by §21, and suppose that, for example, $\alpha_{14} \neq 0$. Transforming S by $O^{\alpha, \beta, \gamma}_{2, 3, 4}$, we obtain a substitution S' in which

$$\alpha'_{11} \equiv \alpha_{11}, \quad \alpha'_{12} \equiv \alpha\alpha_{12} + \beta\alpha_{13} + \gamma\alpha_{14}.$$

To prove that there exists in the $GF[p^n]$ a set of solutions of

$$\beta\alpha_{13} + \gamma\alpha_{14} = \tau, \quad \alpha^2 + \beta^2 + \gamma^2 = 1,$$

we combine them into the single relation

$$\beta^2(\alpha^2_{13} + \alpha^2_{14}) - 2\beta\tau\alpha_{13} + \alpha^2\alpha^2_{14} = \alpha^2_{14} - \tau^2.$$

For $\alpha^2_{13} + \alpha^2_{14} = 0$, and therefore $\alpha_1 \neq 0$, a set of solutions is given by $\alpha = 0$ when $\tau \neq 0$ and by $\alpha = 1$, $\beta = 0$ when $\tau = 0$.

For $\alpha_{13}^2 + \alpha_{14}^2 \neq 0$, there exist solutions of the equivalent equation of condition

$$\{\beta(\alpha_{13}^2 + \alpha_{14}^2) - \tau\alpha_{13}\}^2 + \alpha^2\alpha_{14}^2(\alpha_{13}^2 + \alpha_{14}^2) = \alpha_{14}^2(\alpha_{13}^2 + \alpha_{14}^2 - \tau^2).$$

23. Theorem: *From a substitution S of I in which α_{12} has an arbitrary value we can obtain one in which $1 - \alpha_{11}^2$ is a square, not zero, in the $GF[p^n]$.*

The required substitution belonging to I is the following:

$$S^{-1}C_1C_2SC_1C_2 \equiv S_a C_1 C_2,$$

where S_a denotes the substitution of period two,

$$\xi_i' = \xi_i - 2\alpha_{i1}\left(\sum_{j=1}^{m-1}\alpha_{j1}\xi_j + \mu\alpha_{m1}\xi_m\right) - 2\alpha_{i2}\left(\sum_{j=1}^{m-1}\alpha_{j2}\xi_j + \mu\alpha_{m2}\xi_m\right).$$
$$(i = 1, 2, \ldots, m)$$

The coefficient of ξ_1 in ξ_1' in the product $S_aC_1C_2$ is

$$\bar{\alpha}_{11} \equiv -(1 - 2\alpha_{11}^2 - 2\alpha_{12}^2).$$

Since α_{12} is arbitrary, $\bar{\alpha}_{11}$ takes $(p^n + 1)/2$ distinct values in the field. But, by §4, the number of squares ξ^2 for which $1 - \xi^2$ is a not-square is $(p^n - 1)/4$ or $(p^n - 3)/4$ according as -1 is a square or not-square in the $GF[p^n]$, a result which follows immediately since $\nu\eta^2 + \xi^2 = 1$ has $p^n \pm 1 - 2$ sets of solutions for which the not-square $\nu\eta^2 \neq 0$. Hence $1 - \bar{\alpha}_{11}^2$ takes at least one value other than a not-square. The theorem is therefore proven unless $\bar{\alpha}_{11}^2 = 1$. But if we start from a substitution in which $\alpha_{11}^2 = 1$, we derive a substitution in which $\bar{\alpha}_{11} = 1 + 2\alpha_{12}^2$, and therefore

$$1 - \bar{\alpha}_{11}^2 = -4(\alpha_{12}^2 + 1)\alpha_{12}^2,$$

which, by choice of α_{12}, can be made a square when $p^n \neq 5$. Indeed, we can determine $\alpha_{12} \neq 0$ and σ such that $-1 - \alpha_{12}^2 = \sigma^2 \neq 0$; for there are $p^n - \varepsilon$ sets of solutions in the $GF[p^n]$ of

$$-1 = \alpha_{12}^2 + \sigma^2,$$

ε being ± 1 according as -1 is a square or a not-square. Hence there are $p^n - 5$ or $p^n + 1$ sets of solutions in which $\alpha_{12} \neq 0$, $\sigma \neq 0$.

For $p^n = 5$, the value $\alpha_{12} = 1$ makes $\bar{\alpha}_{11} = 3$, $\bar{\alpha}_{11}^2 = -1$. Using this value for α_{11}, we obtain a substitution in which

$$\bar{\alpha}_{11} = -(1 + 2 - 2\alpha_{12}^2) = 0 \text{ for } \alpha_{12} = 2.$$

24. Theorem: If $m = 4$, $s = 3$, *the group I contains a substitution in which α_{12} is an arbitrary mark in the $GF[p^n]$, or else a substitution affecting only two indices.*

We have the relation between the coefficients of S,

$$\alpha_{11}^2 + \alpha_{12}^2 + \alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2 = 1. \qquad (\nu = \text{not-square})$$

(1). Suppose first that $\alpha_{11}^2 = 1$. Transforming S by

$$O_{2,\,4}^{\alpha,\,-\beta}, \qquad \left(\alpha^2 + \frac{1}{\nu}\beta^2 = 1\right)$$

we obtain a substitution replacing ξ_1 by

$$\alpha_{11}\xi_1 + \left(\alpha\alpha_{12} - \frac{\beta}{\nu}\alpha_{14}\right)\xi_2 + \alpha_{13}\xi_3 + (\beta\alpha_{12} + \alpha\alpha_{14})\,\xi_4.$$

If $\alpha_{12}^2 + \frac{1}{\nu}\alpha_{14}^2$ is a not-square and therefore $\alpha_{13} \neq 0$, we can make $\alpha_{12}' = 0$ by taking

$$\alpha = \frac{\beta}{\nu}\,\frac{\alpha_{14}}{\alpha_{12}}, \quad \beta\left(\alpha_{12}^2 + \frac{1}{\nu}\alpha_{14}^2\right) = \nu\alpha_{12}^2.$$

From a substitution in which $\alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2 = 0$, $\alpha_{12} = 0$, we can obtain, by transformation by $O_{3,\,4}^{\alpha,\,\beta}$, a substitution in which α_{13}' has an arbitrary value τ. Indeed, the values

$$\alpha = \frac{\tau^2 + \alpha_{13}^2}{2\tau\alpha_{13}}, \quad \beta = \frac{\nu(\tau^2 - \alpha_{13}^2)}{2\tau\,\alpha_{14}}$$

make

$$\alpha_{12}' \equiv \alpha\alpha_{13} + \frac{\beta}{\nu}\alpha_{14} = \tau, \;\; \alpha^2 + \frac{1}{\nu}\beta^2 = 1.$$

Transforming by $T_{23}C_3O_{34}^{\kappa,\,\sigma}$, which by proper choice of the last factor belongs to H, we obtain a substitution in which $\alpha_{12}' = \tau$. The same result follows if $\alpha_{12}^2 + \frac{1}{\nu}\alpha_{14}^2 = 0$.

If $\alpha_{12}^2 + \frac{1}{\nu}\alpha_{14}^2$ is a square, we can make $\alpha'_{14} = 0$ by taking

$$\alpha^2\left(\alpha_{12}^2 + \frac{1}{\nu}\alpha_{14}^2\right) = \alpha_{12}^2, \quad \beta = \frac{-\alpha\alpha_{14}}{\alpha_{12}}.$$

With $\alpha_{14} = 0$, we have $\alpha_{12}^2 + \alpha_{13}^2 = 0$. Transforming by $O_{2,\,3}^{\alpha,\,\beta}$ we can, as above, make $\alpha_{12} = \tau$, an arbitrary mark $\neq 0$.

The substitution $S^{-1} C_1 C_2 S C_1 C_2$, as shown in §23, has the coefficient $\bar{\alpha}_{11} \equiv 1 + 2\alpha_{12}^2$, since $\alpha_{11}^2 = 1$. Hence $\bar{\alpha}_{11}$ will reduce to ± 1 only when $\alpha_{12}^2 = 0$ or -1. Since we can choose $\tau \neq 0$ such that $\tau^2 \neq -1$, we have a substitution belonging to I in which $\bar{\alpha}_{11}^2 \neq 1$, a case next treated.

(2). Suppose, however, that $\alpha_{11}^2 \neq 1$. Then, since

$$\alpha_{12}^2 + \alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2 \neq 0,$$

we can determine a substitution O_{234}, as in §12, which will transform S into a substitution having $\alpha_{12} = 0$. If $\alpha_{13} = 0$, we can at once make $\alpha'_{12} = \tau$, as in §22. If $\alpha_{13} \neq 0$, we transform S by $O_{2,\,3,\,4}^{\alpha,\,\beta,\,\gamma}$ and make

$$\alpha'_{12} \equiv \alpha\alpha_{12} + \beta\alpha_{13} + \frac{\gamma}{\nu}\alpha_{14} = \tau, \quad \alpha^2 + \beta^2 + \frac{\gamma^2}{\nu} = 1.$$

These relations combine, on eliminating β, into

$$\left\{\gamma\left(\alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2\right) - \tau\alpha_{14}\right\}^2 + \nu\alpha_{13}\left(\alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2\right)\alpha^2 = \nu\,\alpha_{13}^2\left(\alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2 - \tau^2\right),$$

which has $p^n \pm 1$ sets of solutions γ, α in the $GF[p^n]$; indeed, $\alpha_{13}^2 + \frac{1}{\nu}\alpha_{14}^2 \neq 0$.

25. Theorem: *If $m > 4$ or if $m = 4$, $s = 3$, the group I contains a substitution not the identity and replacing ξ_1 by $\alpha_{11}\xi_1 + \alpha_{12}\xi_2$.*

By a repeated application of §21, we can suppose that

$$\alpha_{1m-1} = \alpha_{1m-2} = \dots = \alpha_{15} = \alpha_{14} = 0.$$

By §§22-24, we can suppose that I contains a substitution affecting only ξ_1 and ξ_2, when the theorem is proven, or a substitution in which $1 - \alpha_{11}^2 =$ square. In the latter case,

$$\alpha_{12}^2 + \alpha_{13}^2 + \frac{1}{\mu_d}\alpha_{1m}^2 = 1 - \alpha_{11}^2 \neq 0,$$

so that by §12 we can make $\alpha_{13}=0$. We then have

$$\alpha_{12}^2+\frac{1}{\mu}\alpha_{1m}^2=1-\alpha_{11}^2=\text{square}.$$

Then, as in §24 we can make $\alpha_{1m}=0$, when the theorem is proven.

The substitution reached is neither the identity nor $C_1C_2\ldots\ldots C_m$. Indeed, $1-\alpha_{11}^2\neq 0$. For the case in which S was of the form treated in §20, the substitution reached was C_iC_k.

26. Theorem: *If $m>4$ or if $m=4$, $s=3$, the group I contains a substitution leaving ξ_1 fixed and not the identity.*

The substitution obtained in §25 is evidently a product $O_{1,2}^{\alpha_{11},\alpha_{12}}S_1$, where S_1 leaves ξ_1 fixed.

If S be not commutative with C_1C_2, I contains

$$S^{-1}C_1C_2SC_1C_2=S_1^{-1}C_1C_2S_1C_1C_2=S_1^{-1}C_2S_1C_2\neq 1,$$

which evidently leaves ξ_1 fixed.

If S be commutative with C_1C_2, S_1 is commutative with C_2 and therefore replaces ξ_2 by $\pm\xi_2$. If S_1 be commutative with every $Q_{i,j}^{\alpha,\beta}$ $(i,j=3,\ldots\ldots,m)$, it has, by §28, the form

$$\xi_1'=\xi_1,\quad \xi_2'=\pm\xi_2,\quad \xi_i'=\lambda\xi_i,\qquad (i=3,\ldots\ldots,m)$$

where $\lambda^2=1$. If then $O_{1,2}^{\alpha_{11},\alpha_{12}}$ be either the identity or C_1C_2, S is of the form treated in §20. If $O_{1,2}$ be not of either form, its square is not the identity, so that S^2 is a substitution of I not the identity and leaving $\xi_3,\ldots\ldots,\xi_m$ fixed. If, however, S_1 be not commutativve with $Q_{3,4}^{\alpha,\beta}$, for example, I will contain

$$S^{-1}Q_{3,4}^{-1}SQ_{3,4}\equiv S_1^{-1}Q_{3,4}^{-1}S_1Q_{3,4}\neq 1,$$

which evidently leaves fixed ξ_1 and ξ_2.

27. Theorem: *If $m>4$ or if $m=4$, $s=3$, the group I contains a substitution, not the identity, affecting at most three indices.*

If $s=m-1$, a repeated application of the previous theorem gives a substitution, not the identity, belonging to I, and affecting only three indices.

If $s=m>4$, we obtain by the same theorem a substitution

$$\xi_i'=\sum_{j=1}^{4}\gamma_{ij}\xi_j,\qquad (i=1,2,3,4)$$

not the identity and belonging to I. By §20, we may suppose that $\gamma_{12} \neq 0$. We can make $\gamma_{11}^2 \neq 1$. For, if $\gamma_{11}^2 = 1$, we transform S by $O_{2,\,3}^{\alpha,\,\beta}$, giving a substitution S' in which

$$\gamma'_{11} = \gamma_{11}, \quad \gamma'_{12} = \alpha\gamma_{12} + \beta\gamma_{13}, \quad \gamma'_{13} = -\beta\gamma_{12} + \alpha\gamma_{13}, \quad \gamma'_{14} = \gamma_{14}.$$

At most two of the $p^n \pm 1$ sets of solutions of $\alpha^2 + \beta^2 = 1$ give the same value to γ'_{12}. Hence, if $p^n > 5$, there are at least $4 = \frac{1}{2}(9-1) = \frac{1}{2}(7+1)$ values of γ'_{12}, and therefore values for which γ'^{2}_{12} is neither zero nor -1. Then in the substitution

$$\bar{S} \equiv S'^{-1} C_1 C_2 S' C_1 C_2,$$

the coefficient

$$\bar{\gamma}_{11} \equiv -(1 - 2\gamma'^{2}_{11} - 2\gamma'^{2}_{12})$$

has a value different from ± 1.

For $p^n = 3$, we have by hypothesis $\gamma_{11}^2 = 1$, $\gamma_{12}^2 = 1$. The substitution $S^{-1} C_1 C_2 S C_1 C_2$ will therefore have $\bar{\gamma}_{11} = 0$.

For $p^n = 5$, the equation $\gamma_{12}^2 + \gamma_{13}^2 + \gamma_{14}^2 = 0$ requires that one of the three squares be zero, another $+1$ and the third -1, since all are not zero. Transforming by a substitution of the form $T_{23} T_{24}$ or $T_{23} T_{34}$, if a transformation be necessary at all, we may take $\gamma_{12}^2 = 1$, $\gamma_{13}^2 = -1$, $\gamma_{14}^2 = 0$. Then $\bar{\gamma}_{11} = 3$.

In every case we have in I a quaternary substitution S' in which $\gamma_{11}^2 \neq 1$. It is therefore not commutative with C_1. Hence, m being > 4, I contains

$$S'^{-1} C_1 C_5 S' C_1 C_5 \equiv S'^{-1} C_1 S C_1 \equiv S_\gamma C_1 \neq 1,$$

where S_γ denotes the substitution

$$\xi'_i = \xi_i - 2\gamma_{i1} \sum_{j=1}^{4} \gamma_{j1} \xi_j. \qquad (i = 1, \ldots, 4)$$

We may, by §12, make $\gamma_{41} = 0$, since we have

$$\gamma_{21}^2 + \gamma_{31}^2 + \gamma_{41}^2 = 1 - \gamma_{11}^2 \neq 0.$$

We therefore have a substitution in I affecting only three indices and different from the identity.

28. Lemma: *If a substitution S of G be commutative with $O_{1,\,m}^{\alpha,\,\beta} \neq 1$, it breaks up into the product of a substitution affecting ξ_1 and ξ_m only and a substitution affecting $\xi_2, \ldots, \xi_{m-1}$ only.*

Indeed, the conditions for the identity $O_{1,\,m}^{\alpha,\,\beta} S \equiv S O_{1,\,m}^{\alpha,\,\beta}$ are:

$$\text{(a)}\quad \beta\alpha_{11} = \beta\alpha_{mm}, \quad \beta\alpha_{m1} = -\frac{\beta}{\mu}\alpha_{1m};$$

$$\left.\begin{array}{ll}\text{(b)}\quad (\alpha-1)\alpha_{1j} + \beta\alpha_{mj} = 0, & -\dfrac{\beta}{\mu}\alpha_{1j} + (\alpha-1)\alpha_{mj} = 0, \\ \text{(c)}\quad (\alpha-1)\alpha_{j1} - \dfrac{\beta}{\mu}\alpha_{jm} = 0, & \beta\alpha_{j1} + (\alpha-1)\alpha_{jm} = 0,\end{array}\right\} \quad (j = 2, \ldots, m-1)$$

Since $\alpha^2 + \frac{1}{\mu}\beta^2 = 1$ and $\alpha \neq 1$, $O_{1,\,2}^{\alpha,\,\beta}$ not being the identity, we have for the determinant of the pair of equations (b) and likewise for the pair (c),

$$(\alpha-1)^2 + \frac{1}{\mu}\beta^2 = 2 - 2\alpha \neq 0.$$

Hence must

$$\alpha_{1j} = \alpha_{mj} = \alpha_{j1} = \alpha_{jm} = 0. \qquad (j = 2, \ldots, m-1)$$

Hence $S \equiv S_{1m} S_{23 \ldots m-1}$, where S_{1m} affects only ξ_1 and ξ_m, and $S_{23 \ldots m-1}$ affects only $\xi_2, \ldots, \xi_{m-1}$. Since S leaves invariant

$$\xi_1^2 + \xi_2^2 + \ldots + \xi_{m-1}^2 + \mu\xi_m^2,$$

S_{1m} must leave $\xi_1^2 + \mu\xi_m^2$ invariant, and hence be either $O_{1,\,m}^{\alpha_{11}\alpha_{1m}}$ or its product by C_1. The latter case is evidently excluded except when $O_{1,\,m}^{\alpha,\,\beta} \equiv C_1 C_m$. Indeed, with this exception, $\beta \neq 0$ so that (a) gives new conditions.

A like result follows if S be commutative with $O_{i,\,j}^{\alpha,\,\beta}$ where $i, j < m$.

29. Theorem: *If $m > 4$ or if $m = 4$, $s = 3$, the group I coincides with H.*

For $p^n > 3$, the subgroup of H which affects three indices only is by §§30–31 a simple group. Since I contains one of the substitutions of this simple group, it contains all. Transforming them by the substitutions $T_{ij}T_{ik}$, belonging to H, we obtain every substitution of H affecting three indices. Hence, for $p^n > 3$, I contains all the generators of H.

For $p^n = 3$, $m = s > 4$, I contains one of the substitutions affecting three indices ξ_1, ξ_2, ξ_3, and not the identity, which by §17 are the following eleven:

$$C_iC_j, \quad T_{ij}T_{ik}, \quad T_{ij}T_{ik}C_rC_s. \qquad (i, j, k, r, s = 1, 2, 3)$$

If it contain one of the last two types, I contains its transformed by $C_i C_j$, viz.

$$T_{ij} T_{ik} C_i C_k \text{ or } T_{ij} T_{ik} C_r C_s \,.\, C_i C_k.$$

Hence, in every case, I contains $C_i C_k$, and therefore also every product of two C_i's. Hence I contains

$$T_{12} T_{34} = W^{-1} C_3 C_4 W, \quad W = W^{-1} C_1 C_5 W C_1 C_5.$$

Since the alternating group on $m > 4$ indices is simple, I contains every product $T_{ij} T_{kl}$. Hence $I \equiv H$.

For $p^n = 3$, $m > 3$, $s = m - 1$, the group I contains one of the substitutions, not the identity, of the group G_{12} leaving invariant $\xi_1^2 + \xi_2^2 - \xi_m^2$, which by §17 is the transformed by O of the group G'_{12}, leaving invariant $\xi_1^2 + \xi_2^2 + \xi_m^2$. We have just proven that any substitution of G'_{12} can be combined with its transformed (by substitutions of G'_{12}) so as to give $C_1 C_2$. The same result holds for G_{12} since O transforms $C_1 C_2$ into itself. Hence I contains every $C_i C_j$ $(i, j < m)$. But $V_{1,2,m}^{-1}$ transforms $C_1 C_2$ into $T_{12} C_m$. Hence I contains every $T_{ij} C_m$ $(i, j < m)$. Finally, I contains $V_{1,2,m}$, since

$$V_{1,2,m}^{-1} (T_{12} C_2 C_3 C_m)^{-1} V_{1,2,m} (T_{12} C_2 C_3 C_m) = V_{1,2,m} C_1 C_2.$$

Hence in this case also I coincides with H.

30. Theorem: *The ternary orthogonal group H in the $GF[p^n]$, $p > 2$, having the order $\frac{1}{2} p^n (p^{2n} - 1)$, is simply isomorphic to the group Γ in the $GF[p^n]$ of linear fractional substitutions of determinant unity on one index.*

Let i be a root of the equation $\xi^2 = -1$, so that i belongs to the $GF[p^n]$ or to the $GF[p^{2n}]$ according as -1 is a square or not-square in the $GF[p^n]$.

Introduce in place of ξ_1, ξ_2, ξ_3 the new indices

$$\eta_1 \equiv -i\xi_1, \quad \eta_2 \equiv \xi_2 - i\xi_3, \quad \eta_3 \equiv \xi_2 + i\xi_3,$$

whence
$$\eta_2 \eta_3 - \eta_1^2 \equiv \xi_1^2 + \xi_2^2 + \xi_3^2.$$

The orthogonal substitution

$$S: \quad \xi'_i = \sum_{j=1}^{3} \alpha_{ij} \xi_j \qquad (i = 1, 2, 3)$$

takes the form

$$S_1: \begin{cases} \eta_1' = \alpha_{11}\eta_1 + \frac{1}{2}(\alpha_{13} - i\alpha_{12})\,\eta_2 - \frac{1}{2}(\alpha_{13} + i\alpha_{12})\,\eta_3, \\ \eta_2' = (\alpha_{31} + i\alpha_{21})\,\eta_1 + \frac{1}{2}(\alpha_{22} - i\alpha_{32} + i\alpha_{23} + \alpha_{33})\,\eta_2 + \frac{1}{2}(\alpha_{22} - i\alpha_{32} - i\alpha_{23} - \alpha_{33})\,\eta_3, \\ \eta_3' = (-\alpha_{31} + i\alpha_{21})\,\eta_1 + \frac{1}{2}(\alpha_{22} + i\alpha_{32} + i\alpha_{23} - \alpha_{33})\,\eta_2 + \frac{1}{2}(\alpha_{22} + i\alpha_{32} - i\alpha_{23} + \alpha_{33})\,\eta_3. \end{cases}$$

We proceed to prove that S_1 can be given the form

$$\begin{pmatrix} \alpha\delta + \beta\gamma & \alpha\gamma & \beta\delta \\ 2\alpha\beta & \alpha^2 & \beta^2 \\ 2\gamma\delta & \gamma^2 & \delta^2 \end{pmatrix}, \qquad [\alpha\delta - \beta\gamma = 1] \qquad (8)$$

where $\alpha, \beta, \gamma, \delta$ are complexes of the form $\rho + \sigma i$, ρ and σ being marks of the $GF[p^n]$. The proof will follow for the general substitution S of H, if proven for the generators of H. Indeed, denoting the substitution (8) by $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, we verify the composition formula,

$$\begin{bmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} = \begin{bmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{bmatrix}.$$

Hence the product of two substitutions of the form (8) is again of the form (8), the composition being identical with that for linear fractional substitutions. Expressing the orthogonal substitution $O_{2,\,3}^{\alpha,\,\beta}$ in terms of the indices η_1, η_2, η_3, we obtain the substitution

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \alpha + \beta i & 0 \\ 0 & 0 & \alpha - \beta i \end{pmatrix}, \qquad [(\alpha + \beta i)(\alpha - \beta i) = 1]$$

which need not be of the form (8); whereas its square $Q_{2,\,3}^{\alpha,\,\beta}$ is always of the form (8). The product $O_{1,\,2}^{\alpha,\,\beta} O_{2,\,3}^{\alpha,\,\beta}$ expressed in the indices η_i is

$$\begin{pmatrix} \alpha & -\dfrac{i\beta}{2} & -\dfrac{i\beta}{2} \\ -\beta i(\alpha + \beta i) & \dfrac{\alpha + 1}{2}(\alpha + \beta i) & \dfrac{\alpha - 1}{2}(\alpha + \beta i) \\ -\beta i(\alpha - \beta i) & \dfrac{\alpha - 1}{2}(\alpha - \beta i) & \dfrac{\alpha + 1}{2}(\alpha - \beta i) \end{pmatrix},$$

which is of the form (8), viz. in the above notation

$$\begin{bmatrix} \frac{1}{2}(\alpha + 1 + \beta i) & -\frac{1}{2}(\alpha - 1 + \beta i) \\ \frac{1}{2}(\alpha - 1 - \beta i) & \frac{1}{2}(\alpha + 1 - \beta i) \end{bmatrix}.$$

In particular we have $T_{12}T_{23}$ so expressed. For $T_{12}T_{13}$ we have

$$\begin{pmatrix} 0 & \frac{1}{2} & -\frac{1}{2} \\ i & -i/2 & -i/2 \\ i & i/2 & i/2 \end{pmatrix} \equiv \begin{bmatrix} \frac{1-i}{2} & -\frac{(1-i)}{2} \\ \frac{1+i}{2} & \frac{1+i}{2} \end{bmatrix}.$$

For $p^n = 5$, we have for the generator R:

$$\begin{pmatrix} 1 & \frac{1}{2}(2-i) & -\frac{1}{2}(2+i) \\ 2+i & \frac{1}{2}.3 & \frac{1}{2}(1-2i) \\ -2+i & \frac{1}{2}(1+2i) & \frac{1}{2}3 \end{pmatrix} = \begin{bmatrix} -3 & 3-i \\ 3+i & 3 \end{bmatrix}.$$

Since H can be generated from the above substitutions, it follows that every substitution of H can be put into the form (8).

If -1 be a square, the coefficients α, β, γ, δ belong to the $GF[p^n]$, so that H is simply isomorphic to Γ.

If -1 be a not-square, α and δ, β and γ are conjugate imaginaries in i, so that H is simply isomorphic to the imaginary form* of the group Γ. But Γ is known† to be a simple group if $p^n > 3$.

Corollary. For $m = 3$, the group H does not coincide with G.

31. Theorem: *The subgroup H_ν of the group G_ν of all linear substitutions leaving $\xi_1^2 + \xi_2^2 + \nu\xi_3^2$ invariant is simple if $p^n > 3$.*

Since the substitution

$$O: \begin{cases} \xi_1' = \alpha\xi_1 - \beta\xi_2 \\ \xi_2' = \beta\xi_1 + \alpha\xi_2 \end{cases} \qquad (\alpha^2 + \beta^2 = \nu)$$

transforms $\xi_1^2 + \xi_2^2 + \nu\xi_3^2$ into $\nu(\xi_1^2 + \xi_2^2 + \xi_3^2)$, it transforms G_ν into the ternary orthogonal group G. Further, O transforms C_1C_3, which extends H_ν to G_ν, into $O_{1,\,2}^{\rho,\,\sigma}\, C_1C_3$, where

$$\rho = \frac{\alpha^2 - \beta^2}{\alpha^2 + \beta^2}, \quad \sigma = \frac{2\alpha\beta}{\alpha^2 + \beta^2}, \quad \rho^2 + \sigma^2 = 1.$$

---

*Moore, *A doubly-infinite system of simple groups*, Congress Mathematical Papers, 1893.

†Besides the proof by Moore, the theorem has been established by Burnside in the Proceedings of the London Mathematical Society, 1894, and by Dickson in the Annals of Mathematics, 1897.

The latter substitution serves to extend H to G; indeed $O^{\rho,\sigma}_{1,2}$ is not in the group $Q_{1,2}$ since

$$\frac{1+\rho}{2} \equiv \frac{\alpha^2}{\alpha^2+\beta^2} = \frac{\alpha^2}{\nu}$$

is a not-square, and therefere ρ not of the form $2S^2-1$.

It follows that H_ν is simply isomorphic to H.

Linear homogeneous group in the Galois field of order 2^n *defined by a quadratic invariant*, §§32–48.

32. We will assume that the invariant

$$f \equiv \sum_{i \overline{\overline{<}} j}^{i,j=1 \dots m} \alpha_{ij}\xi_i\xi_j$$

cannot be expressed as a quadratic function of fewer than m variables belonging to the $GF[2^n]$. It will be convenient to set $\alpha_{ji} \equiv \alpha_{ij}$.

Theorem: *We can determine a linear homogeneous substitution belonging to the* $GF[2^n]$ *which will transform* f *into one of the following forms*:

$$(m \text{ odd}) \qquad \xi_1\xi_2 + \xi_3\xi_4 + \dots + \xi_{m-2}\xi_{m-1} + \xi_m^2,$$
$$(m \text{ even}) \qquad \xi_1\xi_2 + \xi_3\xi_4 + \dots + \xi_{m-3}\xi_{m-2} + \alpha\xi_{m-1}^2 + \beta\xi_{m-1}\xi_m + \gamma\xi_m^2.$$

We first prove that, if $m \overline{\overline{>}} 3$, f can be transformed into a quadratic form having $\alpha_{11}=0$. If every α_{ij} $(i,j=1,\dots,m;\ i \neq j)$ were zero, f would have the form

$$f \equiv (\sqrt{\alpha_{11}}\xi_1 + \sqrt{\alpha_{22}}\xi_2 + \dots + \sqrt{\alpha_{mm}}\xi_m)^2.$$

This being contrary to our hypothesis, we may assume that $\alpha_{23} \neq 0$, for example. We may also suppose that $\alpha_{22} \neq 0$, since otherwise the transformed of f by $(\xi_1\xi_2)$ would have $\alpha_{11}=0$. The terms of f which involve ξ_2 may be written thus,

$$\alpha_{22}\xi_2^2 + \xi_2(\alpha_{21}\xi_1 + \alpha_{23}\xi_3 + \alpha_{24}\xi_4 + \dots + \alpha_{2m}\xi_m).$$

Hence the inverse of the following substitution,

$$\xi_3' = \alpha_{21}\xi_1 + \alpha_{23}\xi_3 + \alpha_{24}\xi_4 + \dots + \alpha_{2m}\xi_m,$$
$$\xi_i' = \xi_i \qquad (i=1,\dots,m;\ i \neq 3),$$

will transform f into

$$\alpha_{22}\xi_2^2+\xi_2\xi_3+\Sigma\beta_{ij}\xi_i\xi_j,$$

summed for $i, j=1, 3, 4, \ldots, m$; $i<j$. Applying the substitution

$$\xi_2'=\xi_2+\lambda\xi_1, \quad \xi_i'=\xi_i, \qquad (i=1, 3, 4, \ldots, m)$$

we obtain as the new coefficient of ξ_1^2 the function $\alpha_{22}\lambda^2+\beta_{11}$, which may be made to vanish by determining λ.

We may therefore suppose that $\alpha_{11}=0$ in our original function f. Since the α_{1j} are not all zero, we may assume that $\alpha_{12}\neq 0$. Applying to f the inverse of the substitution

$$\xi_2'=\alpha_{12}\xi_2+\alpha_{13}\xi_3+\ldots+\alpha_{1m}\xi_m, \quad \xi_i'=\xi_i \qquad (i=1, 3, 4, \ldots, m)$$

we obtain the function

$$\xi_1\xi_2+\sum_{i<j}^{i,j=2,\ldots,m}\gamma_{ij}\xi_i\xi_j.$$

Replacing $\xi_1+\gamma_{22}\xi_2+\gamma_{23}\xi_3+\ldots+\gamma_{2m}\xi_m$ by ξ_1, we get

$$f'\equiv\xi_1\xi_2+\sum_{i,j}^{3,\ldots,m}\delta_{ij}\xi_i\xi_j.$$

Similarly, if $m \geqq 5$, we can transform f' into

$$\xi_1\xi_2+\xi_3\xi_4+\sum_{i,j}^{5,\ldots,m}\varepsilon_{ij}\xi_i\xi_j.$$

The theorem follows by a simple induction.

33. Theorem: *For m even, the quadratic invariant can be reduced by a linear substitution in the $GF[2^n]$ to the form*

$$F_\lambda\equiv\xi_1\xi_2+\xi_3\xi_4+\ldots+\xi_{m-1}\xi_m+\lambda\xi_{m-1}^2+\lambda\xi_m^2,$$

where $\lambda=0$ or has any one of the values for which the form $\xi_{m-1}\xi_m+\lambda\xi_{m-1}^2+\lambda\xi_{2m}^2$ is irreducible in the $GF[2^n]$.

If $\alpha\xi_{m-1}^2+\beta\xi_{m-1}\xi_m+\gamma\xi_m^2$ be reducible, the form reached in §32 can evidently be reduced to F_0. In the contrary case, it can readily be given the form

$$\xi_1\xi_2+\xi_3\xi_4+\ldots+\xi_{m-3}\xi_{m-2}+\xi_{m-1}^2+\xi_{m-1}\xi_m+\delta\xi_m^2,$$

δ being such a mark that the equation

$$\xi^2 + \xi + \delta = 0 \tag{9}$$

is irreducible in the $GF[2^n]$. It follows from (9) that

$$\xi^{2^n} = \xi + \delta + \delta^2 + \delta^4 + \ldots + \delta^{2^{n-1}}.$$

Hence (9) has a root ξ in the $GF[2^n]$ if and only if

$$\delta + \delta^2 + \ldots + \delta^{2^{n-1}} = 0.$$

The left member being its own square in the $GF[2^n]$ and hence either 0 or 1, it follows that (9) is irreducible in that field if and only if

$$\delta + \delta^2 + \delta^4 + \ldots + \delta^{2^{n-1}} = 1. \tag{10}$$

Applying to our quadratic form the transformation

$$\xi'_{m-1} = \xi_{m-1} + \lambda\xi_m, \quad \xi'_i = \xi_i, \qquad (i = 1, \ldots, m;\ i \neq m-1)$$

the constant δ is replaced by

$$\delta' \equiv \delta + \lambda + \lambda^2,$$

which is therefore a root of (10). Giving to λ all possible values in the $GF[2^n]$, we obtain the 2^{n-1} roots of (10). Indeed, if in the $GF[2^n]$,

$$\delta + \lambda + \lambda^2 = \delta + \lambda_1 + \lambda_1^2,$$

we must have $\lambda_1 = \lambda$ or $\lambda + 1$. Hence all irreducible quadratic forms in two variables of the $GF[2^n]$ can be transformed linearly into each other. For n odd, we can choose the form given by $\delta = 1$. Applying, finally, the transformation

$$\xi'_{m-1} = \delta^{\frac{1}{2}}\xi_{m-1}, \quad \xi'_m = \delta^{-\frac{1}{2}}\xi'_m, \quad \xi'_i = \xi_i \qquad (i = 1 \ldots m-2)$$

our form becomes $F_{\delta^{\frac{1}{2}}}$.

34. Changing the notation, we proceed to study the group G_λ of linear substitutions belonging to the $GF[2^n]$,

$$S: \begin{cases} \xi'_i = \sum\limits_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta'_i = \sum\limits_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j) \end{cases} \qquad (i = 1, \ldots, m)$$

which leave absolutely invariant the function

$$F_\lambda \equiv \sum_{i=1}^{m} \xi_i \eta_i + \lambda \xi_1^2 + \lambda \eta_1^2 .$$

The conditions on the coefficients are seen to be the following:

$$\left\{ \begin{array}{ll} \sum_{i=1}^{m} (\alpha_{ij}\beta_{ik} + \alpha_{ik}\beta_{ij}) = 0, & \sum_{i=1}^{m} (\gamma_{ij}\delta_{ik} + \gamma_{ik}\delta_{ij}) = 0, \\ \sum_{i=1}^{m} (\alpha_{ij}\delta_{ik} + \gamma_{ik}\beta_{ij}) & = \begin{matrix} 0 \ (j \neq k) \\ 1 \ (j = k) \end{matrix} ; \end{array} \right. \tag{11}$$

$$\left\{ \begin{array}{ll} \sum_{i=1}^{m} \alpha_{ij}\beta_{ij} + \lambda\alpha_{1j}^2 + \lambda\beta_{1j}^2 = & \begin{matrix} 0 \ (j > 1) \\ \lambda \ (j = 1) \end{matrix} , \\ \sum_{i=1}^{m} \gamma_{ij}\delta_{ij} + \lambda\gamma_{1j}^2 + \lambda\delta_{1j}^2 \ = & \begin{matrix} 0 \ (j > 1) \\ \lambda \ (j = 1) \end{matrix} . \end{array} \right. \tag{12}$$

It follows from the conditions (11) that S is an Abelian substitution on $2m$ indices in the $GF[2^n]$ and that its reciprocal is obtained by replacing α_{ij}, β_{ij}, γ_{ij}, δ_{ij} by respectively δ_{ji}, β_{ji} γ_{ji}, α_{ji}. By making this replacement in the relations (11) and (12), we obtain an equivalent set of relations (11_r) and (12_r)

35. Among the simplest substitutions leaving F_λ invariant occur the follow ing [only the indices altered being written]:

$$\begin{array}{lll} N_{i,j,\kappa}: \xi_i' = \xi_i + \kappa\eta_j, & \xi_j' = \xi_j + \kappa\eta_i, \\ R_{i,j,\kappa}: \eta_i' = \eta_i + \kappa\xi_j, & \eta_j' = \eta_j + \kappa\xi_i, \\ Q_{i,j,\kappa}: \xi_i' = \xi_i + \kappa\xi_j, & \eta_j' = \eta_j + \kappa\eta_i, \\ T_{i,\kappa} \ : \xi_i' = \kappa\xi_i \quad , & \eta_i' = \kappa^{-1}\eta_i \quad , \end{array}$$

where $i, j > 1$, if $\lambda \neq 0$;

$$\begin{array}{ll} N_{1,j,\kappa}: \xi_1' = \xi_1 + \kappa\eta_j, & \xi_j' = \xi_j + \kappa\eta_1 + \lambda\kappa^2\eta_j, \\ R_{1,j,\kappa}: \eta_1' = \eta_1 + \kappa\xi_j, & \eta_j' = \eta_j + \kappa\xi_1 + \lambda\kappa^2\xi_j, \\ Q_{1,j,\kappa}: \xi_1' = \xi_1 + \kappa\xi_j, & \eta_j' = \eta_j + \kappa\eta_1 + \lambda\kappa^2\xi_j, \\ Q_{j,1,\kappa}: \eta_1' = \eta_1 + \kappa\eta_j, & \xi_j' = \xi_j + \kappa\xi_1 + \lambda\kappa^2\eta_j, \end{array}$$

which, for $\lambda = 0$, fall under the above types;

$$M_i \equiv (\xi_i \eta_i) \quad , \quad P_{ij} \equiv (\xi_i \xi_j)(\eta_i \eta_j) ,$$
$$L: \quad \xi_1' = \eta_1, \quad \eta_1' = \xi_1 + \lambda^{-1} \eta_1 ,$$

where P_{1j} occurs in G only when $\lambda = 0$.

$$O_1^{\alpha,\,\delta}: \begin{cases} \xi_1' = \alpha \xi_1 + \lambda(\alpha + \delta)\eta_1 , \\ \eta_1' = \lambda(\alpha + \delta)\xi_1 + \delta \eta_1 , \end{cases} \quad [\alpha\delta + \lambda^2(\alpha^2 + \delta^2) = 1] .$$

36. For $\lambda = 0$ our group is the generalized first hypoabelian group G_0; for $\lambda = \lambda'$, where $\xi_1\eta_1 + \lambda'\xi_1^2 + \lambda'\eta_1^2$ is irreducible in the $GF[2^n]$, it is the generalized second hypoabelian group $G_{\lambda'}$. For $n = 1$, the structure of these groups was given by Jordan. The simplifications and corrections introduced by the writer* have been employed in the present paper. As far as practicable we treat together the groups G_0 and $G_{\lambda'}$. We do not completely determine the structure of G_0, that having been done in the paper cited and in more detail in a paper communicated November 10th, 1898, to the London Mathematical Society.

37. Theorem: *The groups G_0 and $G_{\lambda'}$ may be generated as follows:*

$$G_0 \equiv \{M_i,\ N_{i,\,j,\,\kappa}\}, \quad G_{\lambda'} \equiv \{M_i,\ N_{i,\,j,\,\kappa},\ O_1^{\alpha,\,\delta}\},$$

where $i, j = 1, 2, \ldots, m$, and κ is an arbitrary mark in the $GF[2^n]$.

We note that M_i transforms $N_{i,\,j,\,\kappa}$ into $Q_{j,\,i,\,\kappa}$ and $Q_{i,\,j,\,\kappa}$ into $R_{i,\,j,\,\kappa}$. Further, for $i, j > 1$ when $\lambda \neq 0$, we have

$$P_{ij} \equiv Q_{j,\,i,\,1}^{-1}\, Q_{i,\,j,\,1}\, Q_{j,\,i,\,1} ,$$
$$T_{i,\,\mu}\, T_{j,\,\mu} = M_i M_j\, P_{ij}\, R_{i,\,j,\,\mu^{-1}}\, N_{i,\,j,\,\mu}\, R_{i,\,j,\,\mu^{-1}} .$$

But M transforms $T_{j,\,\mu}$ into $T_{j,\,\mu^{-1}}$. Hence the group contains

$$T_{i,\,\mu}\, T_{j,\,\mu} \cdot T_{i,\,\mu}\, T_{j,\,\mu^{-1}} = T_{i,\,\mu^2} .$$

For the case $m = 2$, $\lambda = \lambda'$, the group $G_{\lambda'}$ contains

$$N_{1,\,2,\,\kappa}\, Q_{1,\,2,\,\kappa^{-1}\lambda^{-1}}\, N_{1,\,2,\,\kappa} = L M_1 M_2\, T_{2,\,\lambda\kappa^2} ; \tag{13}$$

and therefore, since $L \equiv O_1^{0,\,\lambda^{-1}}$, it contains every $T_{2,\,\rho}$.

---

* "The Structure of the Hypoabelian Groups," Bulletin of the American Mathematical Society, July, 1898.

To prove that every substitution S satisfying the relations (11) and (12) can be generated from the above substitutions, we first set up a substitution T derived from them which, like S, replaces ξ_m by

$$f \equiv \sum_{j=1}^{m} (\alpha_{mj}\xi_j + \gamma_{mj}\eta_j),$$

where, by (12_r),

$$\sum_{j=1}^{m} \alpha_{mj}\gamma_{mj} + \lambda\alpha_{m1}^2 + \lambda\gamma_{m1}^2 = 0. \tag{14}$$

a). If $\alpha_{mm} \neq 0$, we may take as T the product

$$T_{m\alpha_{mm}} \prod_{i=1}^{m-1} Q_{m,\,i,\,\alpha_{mi}} N_{i,\,m,\,\gamma_{mi}},$$

since it replaces ξ_m by

$$\sum_{j=1}^{m-1} (\alpha_{mj}\xi_j + \gamma_{mj}\eta_j) + \alpha_{mm}\xi_m + \alpha_{mm}^{-1}\Big(\sum_{j=1}^{m-1} \alpha_{mj}\gamma_{mj} + \lambda\alpha_{m1}^2 + \lambda\gamma_{m1}^2\Big)\eta_m,$$

which, by using (14), is seen to be f.

b). If $\alpha_{mm} = 0$, $\gamma_{mm} \neq 0$, we may take as T the product

$$T_{m\gamma_{mm}^{-1}} \prod_{i=1}^{m-1} Q_{i,\,m,\,\gamma_{mi}} R_{i,\,m,\,\alpha_{mi}} \cdot M_1 M_m.$$

c). If $\alpha_{mj} = \gamma_{mj} = 0$ ($j = m, m-1, \ldots, k-1$), but α_{mk} and γ_{mk} not both zero, where $k > 1$, we may obtain, by case (a) or (b), a substitution T' replacing ξ_k by f and derived from the above generators. We may therefore take $T = T'P_{mk}$.

d). If $\alpha_{mj} = \gamma_{mj} = 0$ ($j = m, m-1, \ldots, 2$); the proof given in (c) applies if $\lambda = 0$, so that P_{m1} belongs to the group. For $\lambda = \lambda'$, this case cannot exist, since the equation

$$\alpha_{m1}\gamma_{m1} + \lambda'\alpha_{m1}^2 + \lambda'\gamma_{m1}^2 = 0$$

requires $\alpha_{m1} = \gamma_{m1} = 0$ (whence $f \equiv 0$) on account of the irreducibility in the $GF[2^n]$ of the form $\xi_1\eta_1 + \lambda'\xi_1^2 + \lambda'\eta_1^2$.

It follows that $S = TS_1$, where S_1 leaves ξ_m fixed. Let S_1 replace η_m by

$$f' \equiv \sum_{j=1}^{m} (\beta_{mj}\xi_j + \delta_{mj}\eta_j).$$

Then by (11_r) we have $\delta_{mm} = 1$. Also by (12_r) we have

$$\sum_{j=1}^{m} \beta_{mj}\delta_{mj} + \lambda\delta_{m1}^2 + \lambda\beta_{m1}^2 = 0. \tag{15}$$

Then the product

$$S' \equiv \prod_{i=1}^{m-1} R_{i,\, m,\, \beta_{m1}}\, Q_{i,\, m,\, \delta_{m1}}$$

replaces ξ_m by ξ_m and η_m by

$$\sum_{j=1}^{m-1} (\beta_{mj}\xi_j + \delta_{mj}\eta_j) + \eta_m + \Big(\sum_{j=1}^{m-1} \beta_{mj}\delta_{mj} + \lambda\delta_{m1}^2 + \lambda\beta_{m1}^2\Big)\xi_m,$$

which equals f' since the coefficient of ξ_m is β_{mm} by (15).

We may therefore set $S_1 = S'S_2$, where S_2 leaves ξ_m and η_m fixed. It follows from the relations (11_r) that

$$\alpha_{im} = \beta_{im} = \gamma_{im} = \delta_{im} = 0. \qquad (i = 1, \ldots, m-1)$$

The relations holding between the α_{ij}, β_{ij}, γ_{ij}, δ_{ij} $(i, j = 1, \ldots, m-1)$ are seen to be the relations (11) and (12) written for $m-1$ in place of m. Proceeding with S_2 as we did with S, etc., we find ultimately the result that $S = T'\Sigma$ where T' is derived from the above generators and Σ is a substitution of the group which affects ξ_1 and η_1 only.

38. We next determine the number and nature of the substitutions

$$\Sigma:\quad \xi_1' = \alpha\xi_1 + \gamma\eta_1, \quad \eta_1' = \beta\xi_1 + \delta\eta_1$$

which leave invariant $\xi_1\eta_1 + \lambda\xi_1^2 + \lambda\eta_1^2$. The conditions (11) and (12) become for the present case $(m = 1)$:

$$\alpha\delta + \beta\gamma = 1, \quad \alpha\beta + \lambda\alpha^2 + \lambda\beta^2 = \lambda, \quad \gamma\delta + \lambda\gamma^2 + \lambda\delta^2 = \lambda. \tag{16}$$

Expressing the same conditions for the reciprocal of Σ, we get,

$$\delta\beta + \lambda\delta^2 + \lambda\beta^2 = \lambda, \quad \gamma\alpha + \lambda\gamma^2 + \lambda\alpha^2 = \lambda. \tag{17}$$

Combining (17) with the last two of (16), we find

$$\beta(\alpha+\delta)=\gamma(\alpha+\delta)=\lambda(\alpha+\delta)^2, \tag{18}$$

which may be taken to replace (17).

a). Suppose that $\alpha \neq \delta$. Then by (18)

$$\beta=\gamma=\lambda(\alpha+\delta), \tag{18'}$$

when the conditions (16) all reduce to

$$\alpha\delta+\lambda^2\alpha^2+\lambda^2\delta^2=1. \tag{19}$$

If $\lambda=0$, the substitution Σ becomes $T_{1,\alpha}$. If, however, $\lambda=\lambda'$, so that $\xi_1\xi_2+\lambda\xi_1^2+\lambda\xi_2^2$ is irreducible, the only set of solutions in the $GF[2^n]$ of $\alpha\delta+\lambda^2\alpha^2+\lambda^2\delta^2=0$ is $\alpha=\delta=0$. Each one of the remaining $2^{2n}-1$ sets of values α_1, δ_1 in the $GF[2^n]$ make

$$\alpha_1\delta_1+\lambda^2\alpha_1^2+\lambda^2\delta_1^2=x^2\neq 0.$$

Then will α_1/x, δ_1/x be a set of solutions of (19) and inversely. Hence the number of distinct sets of solutions* of (19) is

$$(2^{2n}-1)/(2^n-1)=2^n+1.$$

b). Suppose next that $\alpha=\delta$, so that the conditions (18) become identities. From the last two of (16) we find that

$$\alpha(\beta+\gamma)=\lambda(\beta+\gamma)^2.$$

*If n be odd, we may take $\lambda=1$. Among the solutions occur

$$(\alpha,\delta)=(0,1),(1,0),(1,1).$$

For $n=1$, there are no other solutions. For $n=3$, we find also

$$(\alpha,\delta)=(\rho,\rho^2),\quad(\rho,\rho^4),\quad(\rho^2,\rho),\quad(\rho^2,\rho^4),\quad(\rho^4,\rho),\quad(\rho^4,\rho^2)$$

where ρ is a definite root of the congruence $\rho^3=\rho+1$, irreducible modulo 2. For $n=5$, we derive from (19)

$$a^{32}=a\delta^{31}+\delta^{32}+\delta^{30}+\delta^{28}+\delta^{24}+\delta^{16}+1=0.$$

But $\delta^{32}+\delta^{30}+\delta^{28}+\delta^{24}+\delta^{16}+1=(\delta+1)^2(\delta^5+\delta^3+\delta^2+\delta+1)^2(\delta^5+\delta^4+\delta^3+\delta+1)^2(\delta^5+\delta^4+\delta^2+\delta+1)^2$. These three quintics irreducible modulo 2 furnish 2.5.3 sets of solutions, which with the above three give 2^5+1 sets.

If $\beta=\gamma$, we find from (16)

$$\alpha^2+\beta^2=1,\ \alpha\beta=0.$$

Hence Σ is either the identity or $M_1\equiv(\xi_1\eta_1)$.

If $\beta\neq\gamma$, then $\alpha=\lambda(\beta+\gamma)$ and all the relations (16) reduce to

$$\beta\gamma+\lambda^2\beta^2+\lambda^2\gamma^2=1.$$

By interchanging α with γ and β with δ, the present relations take the form (18′) and (19), which lead to the substitution Σ_1, we will say. Hence the present substitution Σ is the product $M_1\Sigma_1$. The total number of substitutions leaving $\xi_1\eta_1+\lambda\xi_1^2+\lambda\eta_1^2$ invariant is therefore $2\,(2^n+1)$, if the form be irreducible, and $2\,(2^n-1)$ if it be reducible in the $GF[2^n]$.

39. We can now readily determine the order $\Omega^{(\lambda)}_{m,\,n}$ of G^λ, including the cases $\lambda=0$ and $\lambda=\lambda'$. The number of distinct linear functions f by which the substitutions of G_λ can replace ξ_m is $P^{(\lambda)}_{m,\,n}-1$, if $P^{(\lambda)}_{m,\,n}$ denote the number of sets of solutions in the $GF[2^n]$ of the equation (14). For $m>1$, the pair of equations

$$\alpha_{mm}\gamma_{mm}=\tau,\quad \sum_{j=1}^{m-1}\alpha_{mj}\gamma_{mj}+\lambda\alpha^2_{m1}+\lambda\gamma^2_{m1}=\tau$$

has $(2^{n+1}-1)\,P^{(\lambda)}_{m-1,\,n}$ sets of solutions when $\tau=0$ and $(2^n-1)(2^{n\,(2m-2)}-P^{(\lambda)}_{m-1,\,n})$ sets of solutions when τ runs through the marks $\neq 0$ of the $GF[2^n]$. Hence we have the recursion formula,

$$P^{(\lambda)}_{m,\,n}=2^nP^{(\lambda)}_{m-1,\,n}+(2^n-1)\,2^{n\,(2m-2)}. \tag{20}$$

For $\lambda=0$, $P^{(0)}_{1,\,n}=2\,(2^n-1)$ and we find by induction that

$$P^{(0)}_{s,\,n}-1=(2^{ns}-1)(2^{n\,(s-1)}+1).$$

For $\lambda=\lambda'$, $P^{(\lambda')}_{1,\,n}=1$, since $\alpha=\gamma=0$ is the only set of solutions in the $GF\,[2^n]$ of $\alpha\gamma+\lambda'\alpha^2+\lambda'\gamma^2=0$. We prove by induction that

$$P^{(\lambda')}_{s,\,n}-1=(2^{ns}+1)(2^{n\,(s-1)}-1).$$

The number of distinct linear functions f' is $2^{n\,(2m-2)}$. Indeed, since $\delta_{mm}=1$, the relation (15) determines β_{mm} in terms of β_{mj}, δ_{mj} $(j=1,\ldots\ldots,m-1)$, which may be chosen arbitrarily in the $GF\,[2^n]$. It follows, therefore, from §37, that

$$\Omega^{(\lambda)}_{m,\,n}=(P^{(\lambda)}_{m,\,n}-1)\,2^{2n\,(m-1)}\Omega^{(\lambda)}_{m-1,\,n}.$$

But, by §38, we have the initial values

$$\Omega^{(0)}_{1,n} = 2(2^n - 1), \quad \Omega^{(\lambda')}_{1,n} = 2(2^n + 1).$$

We now readily obtain the formulæ

$$\Omega^{(0)}_{m,n} = (2^{nm}-1)[(2^{2n(m-1)}-1)\,2^{2n(m-1)}][(2^{2n(m-2)}-1)\,2^{2n(m-2)}]\ldots\ldots[(2^{2n}-1)\,2^{2n}]\,2,$$
$$\Omega^{(\lambda')}_{m,n} = (2^{nm}+1)[(2^{2n(m-1)}-1)\,2^{2n(m-1)}]\ldots\ldots[(2^{2n}-1)\,2^{2n}]\,2.$$

40. In determining the structure of G_λ, we shall find that there exists a subgroup J_λ characterized by the additional relation between the coefficients

$$I(\alpha, \beta, \gamma, \delta) \equiv \sum_{i,j}^{1\ldots\ldots m} \alpha_{ij}\delta_{ij} + \lambda^2(\alpha_{11}^2 + \beta_{11}^2 + \gamma_{11}^2 + \delta_{11}^2) = m. \tag{21}$$

We shall prove that all the substitutions of G_λ which satisfy (21) form a group and that this group can be generated as follows:

$$J_0 \equiv \{M_iM_j,\ N_{i,j,\kappa}\}, \quad J_{\lambda'} \equiv \{M_iM_j,\ N_{i,j,\kappa},\ O_1^{\alpha,\delta}\},$$

new generators, as $T_{1,\kappa}$ and $Q_{1,2,\kappa}$ being necessary in J_0 if $m = 2$ [see note to §50].

We first prove that every substitution of the group J_λ satisfies the relation (21). It is evidently satisfied by the generators; for example, for $O_1^{\alpha,\delta}$ we find

$$I(\alpha, \beta, \gamma, \delta) = (m-1) + \alpha\delta + \lambda^2(\alpha^2 + \delta^2) \equiv m \pmod{2}.$$

To give a proof by induction, we suppose that a substitution Σ satisfies (21) and prove that the products $M_iM_j\Sigma$, $N_{i,j,\kappa}\Sigma$, $O_1^{\alpha,\delta}\Sigma$ will satisfy (21), whereas the product $M_j\Sigma$ will not.

a). The coefficients $\bar{\alpha}_{ij}$, $\bar{\beta}_{ij}$, ..., of $M_j\Sigma$ are as follows:

$$\bar{\alpha}_{ij} = \gamma_{ij}, \quad \bar{\gamma}_{ij} = \alpha_{ij}, \quad \bar{\beta}_{ij} = \delta_{ij}, \quad \bar{\delta}_{ij} = \beta_{ij}, \qquad (i = 1, \ldots\ldots, m)$$
$$\bar{\alpha}_{ik} = \alpha_{ik}, \quad \bar{\beta}_{ik} = \beta_{ik}, \quad \bar{\gamma}_{ik} = \gamma_{ik}, \quad \bar{\delta}_{ik} = \delta_{ik}. \quad \begin{pmatrix} i = 1, \ldots\ldots, m \\ k = 1, \ldots\ldots, m; k \neq j \end{pmatrix}$$

Hence

$$I(\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta}) = \sum_{k \neq j}^{i,k=1\ldots\ldots m} \alpha_{ik}\delta_{ik} + \sum_{i=1}^{m} \gamma_{ij}\beta_{ij} + \lambda^2(\alpha_{11}^2 + \beta_{11}^2 + \gamma_{11}^2 + \delta_{11}^2)$$
$$= I(\alpha, \beta, \gamma, \delta) + \sum_{i=1}^{m} (\gamma_{ij}\beta_{ij} - \alpha_{ij}\delta_{ij}) = m + 1.$$

Hence $M_j\Sigma$ does not satisfy (21), while $M_iM_j\Sigma$ does.

b). The coefficients $\bar{\alpha}_{ij}$, etc., of $N_{1,j,\kappa}\Sigma$ are as follows:

$$\begin{array}{lr} \bar{\alpha}_{rs}=\alpha_{rs}, \quad \bar{\beta}_{rs}=\beta_{rs}, & (r, s=1, \ldots, m) \\ \bar{\gamma}_{rs}=\gamma_{rs}, \quad \bar{\delta}_{rs}=\delta_{rs}, & (r, s=1, \ldots, m;\ s\neq 1, j) \\ \bar{\gamma}_{r1}=\gamma_{r1}+\kappa\alpha_{rj}, \quad \bar{\gamma}_{rj}=\gamma_{rj}+\kappa\alpha_{r1}+\lambda\kappa^2\alpha_{rj}, & (r=1, \ldots, m) \\ \bar{\delta}_{r1}=\delta_{r1}+\kappa\beta_{rj}, \quad \bar{\delta}_{rj}=\delta_{rj}+\kappa\beta_{r1}+\lambda\kappa^2\beta_{rj}. & (r=1, \ldots, m) \end{array}$$

Hence $I(\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})$ equals

$$\sum_{s\neq 1,j}^{r,s=1\ldots m}\alpha_{rs}\delta_{rs}+\sum_{r=1}^{m}\alpha_{r1}(\delta_{r1}+\kappa\beta_{rj})+\sum_{r=1}^{m}\alpha_{rj}(\delta_{rj}+\kappa\beta_{r1}+\lambda\kappa^2\beta_{rj})$$
$$+\lambda^2\{\alpha_{11}^2+\beta_{11}^2+(\gamma_{11}+\kappa\alpha_{1j})^2+(\delta_{11}+\kappa\beta_{1j})^2\}$$
$$=\sum_{r,s}^{1\ldots m}\alpha_{rs}\delta_{rs}+\lambda^2(\alpha_{11}^2+\beta_{11}^2+\gamma_{11}^2+\delta_{11}^2)+\kappa\sum_{r=1}^{m}(\alpha_{r1}\beta_{rj}+\alpha_{rj}\beta_{r1})$$
$$+\lambda\kappa^2\Big(\sum_{r=1}^{m}\alpha_{rj}\beta_{rj}+\lambda\alpha_{1j}^2+\lambda\beta_{1j}^2\Big),$$

which equals $I(\alpha, \beta, \gamma, \delta)$ since the last two sums are zero by (11) and (12).

An analogous proof holds for the products $N_{i,j,\kappa}\Sigma$ $(i, j>1)$.

c). The coefficients in the product $O_1^{\alpha,\delta}\Sigma$ are

$$\begin{array}{lr} \bar{\alpha}_{ij}=\alpha_{ij}, \quad \bar{\beta}_{ij}=\beta_{ij}, \quad \bar{\gamma}_{ij}=\gamma_{ij}, \quad \bar{\delta}_{ij}=\delta_{ij}, & (i, j=2, \ldots, m) \\ \bar{\alpha}_{i1}=\alpha\alpha_{i1}+\lambda(\alpha+\delta)\gamma_{i1}, \quad \bar{\gamma}_{i1}=\lambda(\alpha+\delta)\alpha_{i1}+\delta\gamma_{i1}, & \\ \bar{\beta}_{i1}=\alpha\beta_{i1}+\lambda(\alpha+\delta)\delta_{i1}, \quad \bar{\delta}_{i1}=\lambda(\alpha+\delta)\beta_{i1}+\delta\delta_{i1}. & (i=1, \ldots, m) \end{array}$$

Using (11), (12) and (19), we may verify that

$$I(\bar{\alpha}, \bar{\beta}, \bar{\gamma}, \bar{\delta})=I(\alpha, \beta, \gamma, \delta).$$

d). It follows from the remarks at the beginning of §37 that the substitutions $Q_{i,j,\kappa}$, $R_{i,j,\kappa}$ $(i, j=1, \ldots, m)$ and $P_{i,j}$, $T_{i,\kappa}$ $(i, j>1$ if $\lambda=\lambda')$ satisfy the relation (21) and likewise their products by Σ.

Inversely, every substitution S satisfying the relations (11), (12) and (21) *belongs to the group J_λ.*

For $m>2$, the group J_λ contains $Q_{i,j,\kappa}$, the transformed of $N_{i,j,\kappa}$ by M_jM_k $(k\neq i, j)$; also $R_{i,j,\kappa}$ and $Q_{j,i,\kappa}$, the transformed of $N_{i,j,\kappa}$ and $Q_{i,j,\kappa}$

respectively by M_iM_j. Then by §37, it contains P_{ij}, $T_{i,\kappa}T_{j,\kappa}$ $(i, j > 1)$ and $T_{i,\kappa}T_{j,\kappa-1}$, the transformed of the latter by M_1M_j. The product of the two gives T_{i,κ^2}.

For $m = 2$, $\lambda = \lambda'$, the group $J_{\lambda'}$ contains

$$Q_{2,1,\kappa} = L^{-1}N_{1,2,\kappa}L,$$

and therefore $R_{1,2,\kappa}$ and $Q_{1,2,\kappa}$, the transformed of $N_{1,2,\kappa}$ and $Q_{2,1,\kappa}$ respectively by M_1M_2. It thus contains $T_{2,\rho}$ by (13).

By the proof in §§37–38, every substitution of G_λ is of one of the two forms K or KM_1, where K is derived from the M_iM_j, $N_{i,j,\kappa}$, $Q_{i,j,\kappa}$, $R_{i,j,\kappa}$ $(i, j = 1, \ldots, m)$; $O_1^{\alpha,\delta}$, $T_{i,\kappa}$, P_{ij} $(i, j > 1)$. We may therefore state the theorem:

The group G_λ contains a subgroup J_λ of index 2, which M_1 extends to the total group G_λ.

41. Theorem: *The Group $J_{\lambda'}$ may be generated by the substitutions*

$$L,\ M_iM_j,\ N_{i,j,\kappa}. \qquad (i, j = 1, \ldots, m)$$

As it does not readily appear that every $O_1^{\alpha,\delta}$ can be expressed in terms of the above substitutions [which fact is the gist of our theorem], we give a direct proof of the theorem. In contrast to the method of §37, we begin here by considering the indices ξ_1, η_1 which play a special rôle in our group $J_{\lambda'}$. We shall obtain certain results needed in §43.

Let any given substitution S of $J_{\lambda'}$ replace ξ_1 by

$$\sum_{j=1}^{m} (\alpha_{1j}\xi_j + \gamma_{1j}\eta_j),$$

where by (12_r)

$$\sum_{j=1}^{m} \alpha_{1j}\gamma_{1j} + \lambda\alpha_{11}^2 + \lambda\gamma_{11}^2 = \lambda. \tag{22}$$

If α_{1j}, γ_{1j} $(j = 2, \ldots, m)$ are all zero, $Q_{2,1,1}\,Q_{1,2,1}\,S$ will replace ξ_1 by

$$\gamma_{11}\eta_1 + \alpha_{11}\xi_2 + (\gamma_{11} + \lambda\alpha_{11})\,\eta_2,$$

in which α_{11} and $\gamma_{11} + \lambda\alpha_{11}$ are not both zero by (22). We may therefore confine ourselves to substitutions S in which not every α_{1j}, γ_{1j} $(j = 2, \ldots, m)$ is zero, and in particular may assume that $\alpha_{12} \neq 0$.

The product $N_{1,2,\kappa}S$ replaces ξ_1 by

$$\alpha_{11}\xi_1 + (\gamma_{11} + \kappa\alpha_{12})\eta_1 + \alpha_{12}\xi_2 + (\gamma_{12} + \kappa\alpha_{11} + \lambda\kappa^2\alpha_{12})\eta_2 + \dots.$$

We may, by choice of κ, make the coefficient of η_1 zero. Then in $S' \equiv LN_{1,2,\kappa}S$, we have $\alpha_{11}=0$, $\alpha_{12}\neq 0$. As before, the product $N_{1,2,\mu}S' \equiv S''$ will replace ξ_1 by

$$(\gamma_{11} + \mu\alpha_{12})\eta_1 + \alpha_{12}\xi_2 + \dots.$$

By determining μ, we can make the coefficient of η_1 unity. The substitution S'' therefore has

$$\alpha_{11}=0, \quad \gamma_{11}=1, \; \sum_{j=2}^{m}\alpha_{1j}\gamma_{1j}=0, \quad \alpha_{12}\neq 0.$$

It follows, by §37, that there exists a substitution T, derived from

$$M_iM_j, \quad N_{i,j,\kappa}, \quad T_{i,\kappa}, \quad Q_{i,j,\kappa}, \qquad (i, j = 2, \dots, m) \tag{23}$$

which replaces η_2 by $\sum_{j=2}^{m}(\alpha_{1j}\xi_j + \gamma_{1j}\eta_j)$. Hence the product

$$S_1 \equiv M_1M_2Q_{2,1,1}T^{-1}S''$$

will leave ξ_1 fixed.

It follows that the given substitution $S = \Sigma S_1$, where Σ is derived from L, M_iM_j, $N_{i,j,\kappa}$. Let S_1 replace η_1 by

$$\sum_{j=1}^{m}(\beta_{1j}\xi_j + \delta_{1j}\eta_j),$$

where by (11_r) and (12_r)

$$\delta_{11}=1, \quad \sum_{j=1}^{m}\beta_{1j}\delta_{1j} + \lambda\beta_{11}^2 = 0\cdot \tag{24}$$

If $\beta_{1j}=\delta_{1j}=0$ $(j=2,\dots,m)$, then $\beta_{11}=0$ or λ^{-1}. Hence S_1 or $L^{-1}M_1M_2S_1$ respectively will leave ξ_1 and η_1 fixed.

If $\beta_{12}\neq 0$, for example, then $Q_{2,1,\kappa}S_1$ leaves ξ_1 fixed and replaces η_1 by

$$\eta_1 + (\beta_{11} + \kappa\beta_{12})\xi_1 + \beta_{12}\xi_2 + (\delta_{12} + \kappa + \lambda\kappa^2\beta_{12})\eta_2 + \dots.$$

By choice of κ we may make the coefficient of ξ_1 zero. In the resulting substitution S_1', we have

$$\beta_{11}=0, \quad \delta_{11}=1, \; \sum_{j=2}^{m}\beta_{1j}\delta_{1j}=0, \quad \beta_{12}\neq 0.$$

As above, there exists a substitution T' in $J_{\lambda'}$ which replaces η_2 by

$$\sum_{j=2}^{m} (\beta_{1j}\xi_j + \delta_{1j}\eta_j)$$

without altering ξ_1 and η_1. Then will $S_2 \equiv Q_{2,1,1} T'^{-1} S_1'$ leave ξ_1 and η_1 fixed. But, by §37, the substitution S_2 affecting only ξ_i, η_i $(i = 2, \ldots, m)$ can be derived from the substitutions (23).

42. We can make a new determination of the order of $J_{\lambda'}$. The number of sets of solutions of (22) is

$$(2^{2nm} - P_{m,n}^{(\lambda')})/(2^n - 1) \equiv (2^{nm} + 1)\, 2^{n(m-1)},$$

where $P_{m,n}^{(\lambda')} \equiv 2^{n(2m-1)} - 2^{nm} + 2^{n(m-1)}$ is the number of sets of solutions of

$$\sum_{j=1}^{m} \alpha_{1j}\gamma_{1j} + \lambda\alpha_{11}^2 + \lambda\gamma_{11}^2 = 0.$$

By a slight calculation we find that the number of sets of solutions of (24) is $(2^{n(m-1)} + 1)\, 2^{n(m-1)}$. Hence

$$\Omega_{m,n}^{(\lambda')} = (2^{nm} + 1)(2^{n(m-1)} + 1)\, 2^{2n(m-1)}\Omega_{m-1,n}^{(0)},$$

so that from the order of the first hypoabelian group we readily derive that of the second hypoabelian group.

Simplicity of the Group $J_{\lambda'}$, §§43 46.

43. Let I be an invariant subgroup of* $J_{\lambda'}$ containing a substitution S not the identity,

$$S: \begin{cases} \xi_i' = \sum_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta_i' = \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j), \end{cases} \qquad (i = 1, \ldots, m)$$

Proposition I.—*I contains a substitution, not the identity, which leaves ξ_1 fixed.*

---

* In the following paragraphs the subscript λ' will be dropped from $J_{\lambda'}$.

a). If $\gamma_{11} \neq 0$, J contains a substitution T which leaves ξ_1 fixed and replaces η_1 by

$$\sum_{j=1}^{m} (\alpha_{1j}\xi_j + \gamma_{1j}\eta_j).$$

Hence I contains $T^{-1}ST \equiv S_1$ which replaces ξ_1 by η_1.

If S_1 leaves $\xi_2, \eta_2, \xi_3, \eta_3$ unaltered, I will contain its transformed by the following substitution belonging to J:

$$W: \begin{cases} \xi_1' = \xi_2 + \lambda\eta_2 \qquad\qquad\quad , & \eta_1' = \quad \eta_2 + \lambda\xi_3 + \quad \eta_3 \\ \xi_2' = \xi_1 + \lambda\xi_3 + \quad \eta_3 \qquad , & \eta_2' = \lambda\xi_1 + \quad \eta_1 + \lambda^2\xi_3 + \lambda\eta_3, \\ \xi_3' = \eta_1 + \quad \xi_2 + \lambda\eta_2 + \xi_3, & \eta_3' = \lambda\eta_1 + \lambda\xi_2 + \lambda^2\eta_2 + \quad \eta_3. \end{cases}$$

This transformed leaves ξ_1 and η_1 fixed.

In the contrary case, J contains a substitution T, leaving ξ_1 and η_1 fixed but not commutative with S_1; hence I contains $S_1^{-1}T^{-1}S_1T \neq 1$ which leaves ξ_1 fixed. Indeed, comparing the values by which $S_1R_{2,3,\kappa}$ and $R_{2,3,\kappa}S_1$ replace η_3, we must have

$$\xi_2' = (\ )\,\xi_2 + (\ )\,\xi_3,$$

if S_1 be commutative with $R_{2,3,\kappa}$. Comparing the values by which $S_1Q_{3,2,\kappa}$ and $Q_{3,2,\kappa}S_1$ replace ξ_3, we must have

$$\xi_2' = (\ )\,\xi_2 + (\ )\,\eta_3.$$

Hence $\xi_2' = \alpha\xi_2$. If S_1 be commutative with M_2M_3, we have also $\eta_2' = \alpha\eta_2$. Hence $\alpha^2 = 1$ or $\alpha = 1$. Lastly, if S_1 be commutative with P_{23}, we must have

$$\xi_3' = \xi_3, \quad \eta_3' = \eta_3.$$

There remains the case $m = 2$. If $n > 1$, there exists in the $GF[2^n]$ a mark $\varkappa \neq 1$, $\neq 0$. If S be not commutative with $T_{2,\kappa}$, then $S_1^{-1}T_{2\kappa}^{-1}S_1T_{2\kappa}$ is a substitution belonging to I, leaving ξ_1 fixed and different from the identity. If, however, $S_1T_{2\kappa} = T_{2\kappa}S_1$, we readily find that S_1 must have the form

$$\xi_1' = \eta_1, \quad \eta_1' = \xi_1 + \delta_{11}\eta_1, \quad \xi_2' = \alpha\xi_2, \quad \eta_2' = \alpha^{-1}\eta_2.$$

The relation (21) gives $\delta_{11} = \lambda^{-1}$. Hence $S_1 = LT_{2\alpha}$. Since

$$N_{1,2,\kappa}^{-1}T_{2\alpha}N_{1,2,\kappa} = N_{1,2,\kappa+\kappa\alpha^{-1}}\,T_{2\alpha},$$
$$N_{1,2,\kappa}^{-1}LN_{1,2,\kappa} \;\; = LQ_{2,1,\kappa}N_{1,2,\kappa},$$

it follows that $N_{1,2,\kappa}$ transforms S_1 into

$$N_{1,2,\kappa+\kappa a^{-1}} T_{2a} L Q_{2,1,\kappa} N_{1,2,\kappa}.$$

Hence I contains

$$Q_{2,1,\kappa} N_{1,2,\kappa} N_{1,2,\kappa+\kappa a^{-1}} \equiv Q_{2,1,\kappa} N_{1,2,\kappa a^{-1}},$$

in which the coefficient of γ_{11} is zero.

b). $\gamma_{11}=0$. If $\alpha_{1j}=\gamma_{1j}=0$ $(j=2,\ldots,m)$, S leaves ξ_1 fixed. In the contrary case we may suppose that $\alpha_{13}\neq 0$, when $m \gtreqless 3$.

Transforming S by $N_{2,3,\kappa}$ we obtain a substitution S' which replaces ξ_1 by

$$\alpha_{11}\xi_1+\alpha_{12}\xi_2+\alpha_{13}\xi_3+(\gamma_{12}+\varkappa\alpha_{13})\,\eta_2+(\gamma_{13}+\varkappa\alpha_{12})\,\eta_3+\ldots.$$

We may therefore make $\alpha_{12}=\gamma_{12}+\varkappa\alpha_{13}$. Hence in S' we have $\alpha'_{12}=\gamma'_{12}$. Then I contains the substitution

$$S_1=S'^{-1}L^{-1}M_1M_2S'M_1M_2L$$

which leaves ξ_1 fixed. If S_1 reduce to the identity, we find, by comparing the expressions by which S' and $L^{-1}M_1M_2S'M_1M_2L$ replace η_1, that

$$\lambda^{-1}\xi'_1=\lambda^{-1}\delta'_{11}\xi_1+(\beta'_{12}+\delta'_{12})(\xi_2+\eta_2).$$

Then the transformed of S' by $N_{2,3,\kappa}$ will give a substitution $\overline{S}$ which replaces $\lambda^{-1}\xi_1$ by

$$\delta'_{11}\lambda^{-1}\xi_1+(\beta'_{12}+\delta'_{12})(\xi_2+\eta_2+\varkappa\eta_3).$$

Using $\overline{S}$ in place of our given S', the product denoted by S_1 will not be the identity and will leave ξ_1 fixed.

For $m=2$, we may suppose that $\alpha_{12}\neq 0$. Transforming S by $Q_{2,1,\kappa}$ we obtain a substitution S' which replaces ξ_1 by

$$(\alpha_{11}+\varkappa\alpha_{12})\,\xi_1+\alpha_{12}\xi_2+(\gamma_{12}+\lambda\varkappa^2\alpha_{12})\,\eta_2.$$

We may therefore suppose that the coefficient of η_2 is zero. From (12_r) we get $\alpha_{11}=1$, since $\gamma_{12}=\gamma_{11}=0$. Transforming by $T_{2\kappa}$, we may suppose that $\alpha_{12}=1$. Hence we have a substitution S which replaces ξ_1 by $\xi_1+\xi_2$.

The group I therefore contains $S'\equiv S^{-1}R^{-1}_{1,2,\kappa}SR_{1,2,\kappa}$ which replaces ξ_1 by ξ_1. If it be the identity, we find by equating the values by which $SR_{1,2,\kappa}$ and $R_{1,2,\kappa}S$ replace η_1 that

$$\xi'_2=\delta_{12}\xi_1+(\delta_{11}+\lambda\varkappa\delta_{12})\,\xi_2.$$

By (12_r) we have $\delta_{12}=0$; by (11_r), $\delta_{11}=1$. Hence S would be of the form

$$\xi_1'=\xi_1+\xi_2,\quad \eta_1'=\beta_{11}\xi_1+\eta_1+\beta_{12}\xi_2,\quad \xi_2'=\xi_2,\quad \eta_2'=\beta_{21}\xi_1+\eta_1+\beta_{22}\xi_2+\eta_2.$$

The reciprocal of S replaces ξ_1 by $\xi_1+\xi_2$ and may therefore be used in place of S. But S^{-1} is evidently commutative with $R_{1,2,\kappa}$ only if $\beta_{11}=0$. Then by (12_r) we have $\beta_{12}=\beta_{21}$. Hence

$$S=R_{1,2,\beta_{12}}Q_{1,2,1}.$$

This is transformed by L into

$$S_1\equiv R_{1,2,1+\lambda^{-1}\beta_{12}}Q_{1,2,\beta_{12}}.$$

Hence if $\beta_{12}=0$, I contains $R_{1,2,1}$ which leaves ξ_1 fixed. If $\beta_{12}\neq 0$, we transform S by $T_{2,\beta_{12}^{-1}}$ and obtain

$$S'=R_{1,2,\beta_{12}^2}Q_{1,2,\beta_{12}}$$

Hence I contains $S_1^{-1}S'=R_{1,2,\rho}$ where

$$\rho\equiv 1+\lambda^{-1}\beta+\beta^2\neq 0$$

since the form $\lambda\xi_1^2+\lambda\xi_2^2+\xi_1\xi_2$ is ireducible in the field.

44. Proposition II.— *If* $(m,n)\neq(2,1)$, *the group I contains a substitution, not the identity, which leaves ξ_1 and η_1 fixed.*

We have proven that I contains a substitution S, leaving ξ_1 fixed. Let it replace η_1 by

$$\sum_{j=1}^{m}(\beta_{1j}\xi_j+\delta_{1j}\eta_j),$$

where

$$\delta_{11}=1,\quad \sum_{j=1}^{m}\beta_{1j}\delta_{1j}+\lambda\beta_{11}^2=0. \tag{24}$$

a). If $\beta_{1j}=\delta_{1j}=0$ $(j=2,\ldots,m)$, we proceed as in case (a) of the preceding paragraph. If S leaves $\xi_2,\eta_2,\xi_3,\eta_3$ unaltered, its transform by W will leave ξ_1 and η_1 fixed. In the contrary case J will contain a substitution T, leaving ξ_1 and η_1 fixed and not commutative with S. Hence I contains $S^{-1}T^{-1}ST\neq 1$ which leaves both ξ_1 and η_1 fixed, since S replaces ξ_1 and η_1 by functions of ξ_1 and η_1 only. For $m=2$, $n>1$, I contains a substitution $R_{1,2,\rho}\neq 1$ by the proof in the last paragraph. It therefore contains its transform by $T_{2,\sigma}$, giving

$R_{1,2,\rho\sigma-1}$, and hence contains every $N_{1,2,\kappa}$. Therefore I contains every $Q_{1,2,\kappa}$ and, by (13), every $LM_1M_2T_{2,\lambda\kappa^2}$, and finally, every $T_{2,\rho}$, viz.

$$(LM_1M_2T_{2,\lambda})^{-1}(LM_1M_2T_{2,\lambda\kappa^2}) = T_{2,\lambda\kappa^2+\lambda-1}.$$

The substitution $T_{2,\rho} \neq 1$ leaves ξ_1 and η_1 fixed.

b). If $\beta_{12} \neq 0$, for example, the transformed of S by $T_{2,\beta_{12}}$ gives a substitution S' in which $\beta_{12} = 1$. By §37, J contains a substitution T, leaving ξ_1 and η_1 fixed and replacing ξ_2 by

$$\xi_2 + \tau\eta_2 + \sum_{j=3}^{m} (\beta_{1j}\xi_j + \delta_{1j}\eta_j),$$

the exact value of τ being immaterial here. Then I contains $S_1 \equiv T^{-1}S'T$ which replaces ξ_1 by ξ_1 and η_1 by

$$\beta'_{11}\xi_1 + \eta_1 + \beta'_{12}\eta_2 + \xi_2.$$

b$_1$). If $\beta'_{12} \neq 0$, the transformed S_2 of S_1 by $T_{2,\mu}^{-1}$ will replace η_1 by

$$\beta'_{11}\xi_1 + \eta_1 + \mu(\xi_2 + \eta_2),$$

if we take $\mu = \beta'^{\frac{1}{2}}_{12}$. Let V be any substitution of J which leaves ξ_1, η_1 and $\xi_2 + \eta_2$ fixed. Then $S_3 \equiv S_2^{-1}V^{-1}S_2V$ belongs to I and leaves ξ_1 and η_1 fixed. There remains the case in which S_2 is commutative with every V. If S_2 be commutative with $V = Q_{3,2,\kappa}N_{2,3,\kappa}$, we find, on comparing the two values by which the products S_2V and VS_2 replace ξ_2, that

$$\eta'_3 = \alpha'_{23}(\xi_2 + \eta_2) + (\alpha'_{22} + \gamma'_{22} + \kappa\alpha'_{23})\eta_3.$$

Then, by (12$_r$), $\alpha'_{23} = 0$, so that $\eta'_3 = \delta'_{33}\eta_3$. Taking $V = M_2M_3$, it follows that $\xi'_3 = \delta'_{33}\xi_3$. Hence, by (11$_r$), $\delta'^2_{33} = 1$, so that S_2 leaves ξ_3, η_3 fixed. If $m > 3$, by taking $V = P_{3,i}$, we see that we can suppose that S_2 leaves ξ_i, η_i $(i = 3, \ldots, m)$ fixed. Since S_2 is commutative with M_2M_3, it has the form

$$S_2: \begin{cases} \xi'_1 = \xi_1, \quad \eta'_1 = \beta'_{11}\xi_1 + \eta_1 + \mu(\xi_2 + \eta_2), \\ \xi'_2 = \alpha'_{21}\xi_1 + \alpha'_{22}\xi_2 + \gamma'_{22}\eta_2, \quad \eta'_2 = \alpha'_{21}\xi_1 + \gamma'_{22}\xi_2 + \alpha'_{22}\eta_2. \end{cases}$$

Hence, by (11), $\alpha'^2_{22} + \gamma'^2_{22} = 1$ or $\alpha'_{22} + \gamma'_{22} = 1$, a result found above. By (11) and (21) we find, respectively,

$$\alpha'_{21} = \mu(\alpha_{22} + \gamma_{22}) = \mu, \quad \lambda\beta'_{11} = \alpha'_{22} + 1 = \gamma'_{22}.$$

The transformed of S_2 by $R_{1,2,\kappa}$ gives a substitution which leaves ξ_1 fixed and replaces η_1 by

$$(\beta'_{11}+\kappa^2\gamma'_{22})\xi_1+\eta_1+\ldots.$$

Hence if $\gamma'_{22}\neq 0$, we can make the coefficient of ξ_1 zero. But if $\gamma'_{22}=0$, then $\beta'_{11}=0$. Hence if $m>2$, I contains a substitution, leaving ξ_1 fixed and replacing η_1 by $\eta_1+\beta''_{12}\eta_2+\alpha''_{12}\xi_2$. Then, by (12_r), $\alpha''_{12}\beta''_{12}=0$. Transforming by M_1M_2, if necessary, we can suppose that $\beta''_{12}=0$, so that we are led to case (b_2).

For $m=2$, I contains the substitution S_2,

$$\xi'_1=\xi_1,\quad \eta'_1=\beta_{11}\xi_1+\eta_1+\mu(\xi_2+\eta_2),\quad \xi'_2=\alpha_{21}\xi_1+\alpha_{22}\xi_2+\gamma_{22}\eta_2,\ \text{etc.}$$

We may suppose $\gamma_{22}\neq 0$, since otherwise, $\alpha_{21}=0$ and then $\alpha_{22}=0$ by (11_r). Transforming S_2 by $R_{1,2,\kappa}$ we obtain a substitution in I which leaves ξ_1 fixed and replaces η_1 by

$$(\beta_{11}+\kappa\alpha_{21}+\kappa\mu+\kappa^2\gamma_{22})\xi_1+\eta_1+(\mu+\kappa+\kappa\alpha_{22}+\lambda\mu\kappa^2+\lambda\kappa^3\gamma_{22})\xi_2+(\mu+\kappa\gamma_{22})\eta_2$$

We may therefore make the coefficient of η_2 zero, whence we are led to case (a) or case (b_2).

b_2). If $\beta'_{12}=0$, then $\beta'_{11}+\lambda\beta'^{2}_{11}=0$. Consider the case $m>2$. If J has a substitution T, leaving ξ_1, η_1 and ξ_2 fixed, then $S'_1=S_1^{-1}T^{-1}S_1T$ leaves ξ_1 and η_1 fixed. The proposition therefore follows unless S'_1 is the identity for every possible T. But if S_1 be commutative with $R_{2,3,\kappa}$ and $Q_{3,2,\kappa}$, it must have the form

$$S_1:\ \begin{cases}\xi'_1=\xi_1,\quad \eta'_1=\beta'_{11}\xi_1+\eta_1+\xi_2,\\ \xi'_2=\xi_2,\quad \eta'_2=\xi_1+\beta'_{22}\xi_2+\eta_2+\beta'_{23}\xi_3+\delta'_{23}\eta_3+\ldots,\\ \xi'_3=\delta'_{23}\xi_2+\xi_3,\quad \eta'_3=\beta'_{23}\xi_2+\eta_3.\\ \ldots\ldots\ldots\ldots\ldots\ldots\end{cases}$$

If $m>3$, by supposing S_1 commutative with $R_{3,4,\kappa}$, $Q_{4,3,\kappa}$, etc., we readily see that it reduces to a substitution affecting only ξ_1, η_1, ξ_2, η_2, leading to the case $m=2$, treated below.

If $m=3$, $n>1$, a mark $\kappa\neq 0,\neq 1$ exists in the $GF[2^n]$. If S_1 be commutative with $T_{3,\kappa}$, then $\delta'_{23}=\beta'_{23}=0$, so that we are led to the case $m=2$.

If $m=3$, $n=1$, we have $\beta_{11}=0$ by (21). The product $S_2\equiv M_1M_3S_1M_1M_3S_1$ replaces ξ_3 and η_3 by respectively

$$\xi_3+(\beta'_{23}+\delta'_{23})\xi_2,\quad \eta_3+(\beta'_{23}+\delta'_{23})\xi_2.$$

If $\beta'_{23} = \delta'_{23} = 0$ or 1, we have in S_2 a substitution belonging to I, different from the identity, and leaving ξ_3 and η_3 fixed. If one be zero and the other 1, then S_2 has $\beta''_{23} = \delta''_{23} \equiv \beta'_{23} + \delta'_{23} = 1$. Taking this S_2 in place of our previous S, we evidently obtain the desired result.

For $m = 2$, the substitution S_1, leaving ξ_1 fixed and replacing η_1 by $\beta_{11}\xi_1 + \eta_1 + \xi_2$, where $\beta_{11} = 0$ or λ^{-1}, has for $\beta_{11} = \lambda^{-1}$, the form $S_2 \equiv M_1 M_2 L T_{2,\,\alpha} Q_{2,\,1,\,\alpha}$ and for $\beta_{11} = 0$ the form $S_3 \equiv R_{1,\,2,\,1} T_{2\alpha}$. But $T_{2\rho}$ transforms S_2 into $S'_2 \equiv M_1 M_2 L T_{2,\,\alpha\rho^2} Q_{2,\,1,\,\alpha\rho}$. Hence I contains

$$S_2^{-1} S'_2 \equiv Q_{2,\,1,\,\alpha} T_{2,\,\rho^2}\, Q_{2,\,1,\,\alpha\rho} \equiv T_{2,\,\rho^2} Q_{2,\,1,\,\alpha\rho^2+\alpha\rho}\,.$$

Transforming by $T_{2,\,\alpha\rho}^{-1}$, we get $T_{2,\,\rho^2} Q_{2,\,1,\,\rho+1}$. This $R_{1,\,2,\,\kappa}$ transforms into $R_{1,\,2,\,\kappa(\rho^2+1)} T_{2,\,\rho^2} Q_{2,\,1,\,\rho+1}$. Hence I contains $R_{1,\,2,\,\kappa(\rho^2+1)} \neq 1$, if $\rho \neq 1,\ \neq 0$, as we may assume if $n > 1$.

Similarly, the transformed of S_3 by $R_{1,\,2,\,1}$ gives $R_{1,\,2,\,1} T_{2,\,\alpha} R_{1,\,2,\,\alpha-1}$. Hence I contains $R_{1,\,2,\,\alpha-1}$. Then, as in case (a), I contains a $T_{2,\,\kappa} \neq 1$.

45. Proposition III.—*If* $m > 2$, *the group* I *contains one of the substitutions* $N_{i,\,j,\,\kappa}$ $(i, j > 1)$, *not the identity.*

If $m - 1 > 2$, the group $J^{(m-1)}$, composed of all the substitutions of J which leave ξ_1 and η_1 fixed, is a simple* group. Therefore the group I, have one such substitution, has all.

For the case $m - 1 = 2$, it follows that I contains $N_{2,\,3,\,\kappa}$ or else $P_{23} Q_{3,\,2,\,1}$. The existence of a third pair of indices was assumed in §8 of the paper cited only in transforming by a product of two M_i's or in deriving from $P_{12} Q_{2,\,1,\,1}$ a substitution $Q_{3,\,1,\,1}$ [in case (I_b) of p. 501]. The former operations are allowable in the present investigation since $M_1 M_2$, $M_1 M_3$ belong to our group J.

Transforming $P_{23} Q_{3,\,2,\,1}$ by $T_{3,\,\kappa}$, we get $T_{3,\,\kappa}^{-1} P_{23} T_{3,\,\kappa} Q_{3,\,2,\,\kappa}$. Hence I contains the product

$$P_{23} T_{2,\,\kappa}^{-1} T_{3,\,\kappa} Q_{3,\,2,\,\kappa} \cdot Q_{3,\,2,\,1} P_{23}\,,$$

and therefore its transformed by P_{23}, giving

$$S_4 \equiv T_{2,\,\kappa-1}\, T_{3,\,\kappa} Q_{3,\,2,\,\kappa+1}\,.$$

---

*Dickson, "The Structure of the Hypoabelian Groups," Bulletin of the American Mathematical Society, July, 1898.

If $\varkappa \neq 1$, as we may suppose if $n > 1$, this substitution is not the identity; similarly for the product

$$S_4^{-1} T_{3\kappa}^{-1} S_4 T_{3\kappa} \equiv Q_{3,\,2,\,(\kappa+1)^2}.$$

For the case $n = 1$, we refer to the computation of §18 of the paper cited, where it is proven that I contains $Q_{3,\,2,\,1}$.

46. We may now prove directly that the invariant subgroup I contains the generators L, $M_i M_j$, $N_{i,\,j,\,\kappa}$ of J, so that J is simple.

For $m > 2$, we employ the substitution* derived from the W of §44,

$$V \equiv T_{3,\,\lambda^{-\frac{1}{2}}} T_{2,\,\lambda^{\frac{1}{2}}} W M_1 M_2,$$

$$V: \begin{cases} \xi_1' = \lambda^{-\frac{1}{2}} \eta_2 + \lambda^{\frac{1}{2}} (\xi_3 + \eta_3) \quad , & \eta_1' = \lambda^{\frac{1}{2}} (\xi_2 + \eta_2) \quad , \\ \xi_2' = \lambda \xi_1 + \eta_1 + \lambda^{\frac{3}{2}} (\xi_3 + \eta_3) \quad , & \eta_2' = \xi_1 + \lambda^{\frac{1}{2}} (\xi_3 + \eta_3) \quad , \\ \xi_3' = \eta_1 + \lambda^{\frac{1}{2}} (\xi_2 + \eta_2) + \lambda^{-\frac{1}{2}} \xi_3, & \eta_3' = \lambda \eta_1 + \lambda^{\frac{3}{2}} (\xi_2 + \eta_2) + \lambda^{\frac{1}{2}} \eta_3. \end{cases}$$

We verify that V transforms $M_2 M_3$ into $L M_1 M_3 T_{3,\,\lambda^{-1}}$, so that I contains $L M_1 M_3$. Further, I contains the product

$$Q_{2,\,3,\,\lambda^{-1}} P_{23} M_2 M_3 = \begin{cases} \xi_2' = \lambda^{-1} \eta_2 + \eta_3, & \eta_2' = \xi_3 \quad , \\ \xi_3' = \eta_2 \quad , & \eta_3' = \xi_2 + \lambda^{-1} \xi_3, \end{cases}$$

which is transformed by V into the substitution

$$\begin{cases} \xi_1' = \eta_1, \quad \xi_2' = (\lambda + 1) \xi_2 + \lambda^2 \eta_2 + (\lambda^2 + \lambda) \xi_3 + \lambda \eta_3, \\ \eta_1' = \xi_1, \quad \eta_2' = \xi_2 + (\lambda + 1) \eta_2 + (\lambda + 1) \xi_3 + \eta_3, \\ \xi_3' = \xi_2 + \lambda \eta_2 + \lambda \xi_3 + \eta_3, \quad \eta_3' = (\lambda + 1) \xi_2 + (\lambda^2 + \lambda) \eta_2 + (\lambda^2 + 1) \xi_3 + \lambda \eta_3. \end{cases}$$

This substitution is seen to be the product

$$M_1 M_3 Q_{3,\,2,\,1} N_{3,\,2,\,\lambda} Q_{2,\,3,\,\lambda} R_{2,\,3,\,1}.$$

Hence I contains $M_1 M_3$ and therefore also L. But

$$(L M_1 M_3)^{-1} R_{1,\,2,\,\kappa} (L M_1 M_3) R_{1,\,2,\,\kappa} = Q_{1,\,2,\,\lambda^{-1}\kappa}.$$

It follows now that I contains all the generators of J.

For $m = 2$, $n > 1$, we have proven that I contains a $T_{2,\,\rho} \neq 1$. Transforming it by $N_{1,\,2,\,\kappa}$ we obtain (as in §43) the substitution $N_{1,\,2,\,\kappa+\kappa\rho^{-1}} T_{2,\,\rho}$. Hence I

---

*V corresponds to the substitution of Jordan, p. 211, l. 13, denoted by French capital U.

contains $N_{1,2,\kappa+\kappa\rho-1}$, not the identity. Transforming by $T_{2,\sigma}$ we reach every $N_{1,2,\kappa}$. Transforming $N_{1,2,\kappa}$ by L and LM_1M_2 we obtain $Q_{2,1,\kappa}$ and $Q_{1,2,\kappa}$ respectively. As in §44, case (a), I contains every $T_{2,\kappa}$. By (13) it contains LM_1M_2. If $n>1$, we may assume that $\lambda \neq 1$. Setting $\tau = \dfrac{1}{1+\lambda}$, we find

$$Q_{2,1,1}Q_{1,2,1}T_{2\lambda}Q_{2,1,1}Q_{1,2,1} = LR_{1,2,\tau}Q_{2,1,\tau^{-1}}T_{2,\tau^2},$$

Hence I contains L and therefore M_1M_2. Hence $I \equiv J$.

For $m=2$, $n=1$, the group* J is the simple icosahedral group of order 60.

Linear homogeneous group Γ *in the* $GF[2^n]$ *in* $2m+1$ *indices, defined by a quadratic invariant,* §§47–48.

47. By §32, we may give the invariant the canonical form

$$\psi \equiv \xi_0^2 + \sum_{i=1}^{m} \xi_i \eta_i .$$

The conditions that a substitution

$$S: \quad \begin{cases} \xi_i' = \varkappa_i \xi_0 + \sum_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta_i' = \sigma_i \xi_0 + \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j), \\ \xi_0' = \varkappa_0 \xi_0 + \sum_{j=1}^{m} (\alpha_{0j}\xi_j + \gamma_{0j}\eta_j), \end{cases} \qquad (i=1,2,\ldots\ldots,m)$$

shall leave ψ absolutely invariant are seen to be the relations (11) of §34, together with the following:

$$\sum_{i=1}^{m} (\varkappa_i\beta_{ik} + \sigma_i\alpha_{ik}) = 0, \quad \sum_{i=1}^{m} (\varkappa_i\delta_{ik} + \sigma_i\gamma_{ik}) = 0, \qquad (25)$$

$$(k=1,2,\ldots\ldots,m)$$

$$\alpha_{0j}^2 = \sum_{i=1}^{m} \alpha_{ij}\beta_{ij}, \quad \gamma_{0j}^2 = \sum_{i=1}^{m} \gamma_{ij}\delta_{ij}, \quad \varkappa_0^2 + \sum_{i=1}^{m} \varkappa_i\sigma_i = 1. \qquad (25')$$

---

* Bulletin of the American Math. Soc., pp. 508–9, July, 1898.

It is known* that, for every set of solutions α_{ij}, β_{ij}, γ_{ij}, δ_{ij} in the $GF[2^n]$ of the relations (11), there exists an Abelian substitution

$$\Sigma: \begin{cases} \xi_i' = \sum_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta_i' = \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j) \end{cases} \qquad (i = 1, \ldots, m)$$

of determinant $\Delta \neq 0$ in the field. It is interesting to verify directly that $\Delta \neq 0$. Indeed, suppose that

$$\Delta \equiv \begin{vmatrix} \alpha_{11} & \gamma_{11} & \ldots & \alpha_{1m} & \gamma_{1m} \\ \beta_{11} & \delta_{11} & \ldots & \beta_{1m} & \delta_{1m} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \gamma_{m1} & \ldots & \alpha_{mm} & \gamma_{mm} \\ \beta_{m1} & \delta_{m1} & \ldots & \beta_{mm} & \delta_{mm} \end{vmatrix} = 0.$$

We could then suppose that, for example,

$$\begin{aligned} \gamma_{im} &= \sum_{j=1}^{m} \lambda_j \alpha_{ij} + \sum_{j=1}^{m-1} \mu_j \gamma_{ij}, \\ \delta_{im} &= \sum_{j=1}^{m} \lambda_j \beta_{ij} + \sum_{j=1}^{m-1} \mu_j \delta_{ij}. \end{aligned} \qquad (i = 1, \ldots, m)$$

But these values do not satisfy the relation (11),

$$\sum_{i=1}^{m} \begin{vmatrix} \alpha_{im} & \gamma_{im} \\ \beta_{im} & \delta_{im} \end{vmatrix} = 1.$$

Indeed the left member becomes

$$\sum_{i=1}^{m} \left\{ \sum_{j=1}^{m} \lambda_j \begin{vmatrix} \alpha_{im} & \alpha_{ij} \\ \beta_{im} & \beta_{ij} \end{vmatrix} + \sum_{j=1}^{m-1} \mu_j \begin{vmatrix} \alpha_{im} & \gamma_{ij} \\ \beta_{im} & \delta_{ij} \end{vmatrix} \right\},$$

which, on applying (11), reduces to zero in the $GF[2^n]$.

Since $\Delta \neq 0$, it follows from (25) that

$$x_i = \sigma_i = 0. \qquad (i = 1, \ldots, m)$$

* Dickson, "A Triply-infinite System of Simple Groups," The Quarterly Journal, 1897.

Indeed the determinant of the coefficients of the $2m$ linear homogeneous equations (25) is seen to equal Δ. Hence S takes the form

$$S:\quad \begin{cases} \xi_i' = \sum_{j=1}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta_i' = \sum_{j=1}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j), \\ \xi_0' = \xi_0 + \sum_{j=1}^{m} \left\{ \left(\sum_{i=1}^{m} \alpha_{ij}\beta_{ij} \right)^{\frac{1}{2}} \xi_j + \left(\sum_{i=1}^{m} \gamma_{ij}\delta_{ij} \right)^{\frac{1}{2}} \eta_j \right\}, \end{cases} \qquad (i = 1, \ldots, m)$$

the coefficients being subject to the relations (11) alone. The group of substitutions S is therefore simply isomorphic to the Abelian group of substitutions Σ on $2m$ indices in the $GF[2^n]$. Its structure was determined in the paper cited except when $m = 2$, $n > 1$, in which case the group may be proven to be simple.*

48. Another proof of this result consists in the determination of that subgroup of the first hypoabelian group G_0, leaving $\sum_{i=0}^{m} \xi_i\eta_i$ invariant, for which also the relation $\xi_0 = \eta_0$ is invariant.

In the general substitution of G_0,

$$T:\quad \begin{cases} \xi_i' = \sum_{j=0}^{m} (\alpha_{ij}\xi_j + \gamma_{ij}\eta_j), \\ \eta_i' = \sum_{j=0}^{m} (\beta_{ij}\xi_j + \delta_{ij}\eta_j) \end{cases} \qquad (i = 0, 1, \ldots, m)$$

we must have

$$\beta_{0j} = \alpha_{0j}, \quad \gamma_{0j} = \delta_{0j}, \quad \alpha_{00} + \gamma_{00} = \beta_{00} + \delta_{00}. \qquad (j = 1, \ldots, m)$$

But the inverse to T is

$$T^{-1}:\quad \begin{cases} \xi_i' = \sum_{j=0}^{m} (\delta_{ji}\xi_j + \gamma_{ji}\eta_j), \\ \eta_i' = \sum_{j=0}^{m} (\beta_{ji}\xi_j + \alpha_{ji}\eta_j). \end{cases} \qquad (i = 0, 1, \ldots, m)$$

Putting $\xi_0 = \eta_0$, we find for the coefficients of ξ_0 in ξ_i' and η_i',

$$\delta_{0i} + \gamma_{0i} \equiv 0, \quad \beta_{0i} + \alpha_{0i} \equiv 0. \qquad (i = 1, \ldots, m)$$

* Quarterly Journal of Mathematics, 1899, vol. XXX, p. 383.

But every substitution S of the group Γ is the inverse T^{-1} of some substitution T belonging to Γ. Hence in S the coefficients of ξ_0 in ξ_i' and η_i' are all zero. By the remaining hypoabelian conditions we see that T must be an Abelian substitution of the form S at the end of §47.

Study of quaternary groups with quadratic invariants. Isomorphisms with known groups; summary; §§49–56.

49. In virtue of the identity

$$\xi_1^2+\xi_2^2+\ldots+\xi_M^2-\xi_{M+1}^2-\ldots-\xi_{2M}^2\equiv\sum_{i=1}^{M}(\xi_i-\xi_{M+i})(\xi_i+\xi_{M+i}),$$

it follows from §1 that the group $L_{M,\,p^n}$, leaving $\sum_{i=1}^{M} X_iY_i$ invariant, is simply isomorphic to the group $G_{2M,\,p^n}^{(M)}$ if -1 be a not-square in the $GF[p^n]$, i. e. if p^n be of the form $4l-1$, but is simply isomorphic to the orthogonal group $G_{2M,\,p^n}^{(2M)}$ if $p^n=4l+1$.

The structure of the group $L_{M,\,p^n}$ has been determined directly by the writer, and from the isomorphisms obtained in the paper cited,* we derive the following:

Theorem: *The simple groups of order*

$$\tfrac{1}{8}\,\Omega_{6,\,p^n}^{(6)}\equiv\tfrac{1}{4}(p^{5n}-p^{2n})(p^{4n}-1)\,p^{3n}\,(p^{2n}-1)\,p^n$$
$$\equiv\frac{(p^{4n}-1)(p^{4n}-p^n)(p^{4n}-p^{2n})(p^{4n}-p^{3n})}{4\,(p^n-1)},$$

the one derived from the 6*-ary orthogonal group and the other from the general quaternary linear homogeneous group, each in the* $GF[p^n=4l+1]$, *are simply isomorphic. A like result holds for the simple groups of order*

$$\tfrac{1}{4}\,\Omega_{6,\,p^n}^{(5)}\equiv\tfrac{1}{2}(p^{5n}-p^{2n})(p^{4n}-1)\,p^{3n}\,(p^{2n}-1)\,p^n,$$

the one derived from the group $G_{6,\,p^n}^{(5)}$ *and the other from the general quaternary linear homogeneous group, each in the* $GF[p^n=4l-1]$. *Likewise, the simple group* J_0, *a subgroup of index two under the first hypoabelian group on* $m=3$ *pairs of indices,*

* "The Structure of Certain Linear Groups with Quadratic Invariants," Proceedings of the London Mathematical Society, vol. XXX, pp. 70–98, 1899.

and the simple group of quaternary linear homogeneous substitutions of determinant unity in the $GF[2^n]$, *are isomorphic and of orders*

$$(2^{3n}-1)[(2^{4n}-1)\,2^{4n}][(2^{2n}-1)\,2^{2n}] \equiv \frac{(2^{4n}-1)(2^{4n}-2^n)(2^{4n}-2^{2n})(2^{4n}-2^{3n})}{2^n-1}.$$

50. We next determine the structure of the group $L_{2,\,p^n}$, leaving absolutely invariant $\xi_1\eta_1+\xi_2\eta_2$. The two sets of generators on the ruled surface

$$\xi_1\eta_1+\xi_2\eta_2=0$$

are given by the two pairs of equations

$$\xi_1+\varkappa\xi_2=0, \quad \eta_2-\varkappa\eta_1=0, \tag{26}$$
$$\xi_1+\varkappa\eta_2=0, \quad \xi_2-\varkappa\eta_1=0. \tag{26'}$$

The most general quaternary linear homogeneous substitution, leaving invariant the pair of equations (26), for every value of $\varkappa$ in the field, is readily seen to be

$$\begin{cases} \xi_1'=\alpha\xi_1+\gamma\eta_2, & \xi_2'=-\gamma\eta_1+\alpha\xi_2, \\ \eta_1'=\delta\eta_1-\beta\xi_2, & \eta_2'=\beta\xi_1+\delta\eta_2, \end{cases} \tag{27}$$

having the determinant $(\alpha\delta-\beta\gamma)^2$, For it we have

$$\xi_1'+\varkappa\xi_2'=\alpha(\xi_1+\varkappa\xi_2)+\gamma(\eta_2-\varkappa\eta_1),$$
$$\eta_2'-\varkappa\eta_1'=\beta(\xi_1+\varkappa\xi_2)+\delta(\eta_2-\varkappa\eta_1).$$

The group of the substitutions (27) is therefore simply isomorphic to the binary group on the variables $\xi_1+\varkappa\xi_2$ and $\eta_2-\varkappa\eta_1$. Since the transposition $M_2\equiv(\xi_2\eta_2)$ transforms the pair of equations (26) into the pair (26′), we obtain the most general linear homogeneous substitution, leaving invariant the pair of equations (26′), for every $\varkappa$, if we transform the substitution (27) by M_2, giving

$$\begin{cases} \xi_1'=\alpha\xi_1+\gamma\xi_2, & \xi_2'=\beta\xi_1+\delta\xi_2, \\ \eta_1'=\delta\eta_1-\beta\eta_2, & \eta_2'=-\gamma\eta_1+\alpha\eta_2. \end{cases} \tag{28}$$

The product of an arbitrary substitution (27) and an arbitrary substitution (28) gives

$$\begin{pmatrix} \alpha & 0 & 0 & \gamma \\ 0 & \delta & -\beta & 0 \\ 0 & -\gamma & \alpha & 0 \\ \beta & 0 & 0 & \delta \end{pmatrix} \begin{pmatrix} A & 0 & C & 0 \\ 0 & D & 0 & -B \\ B & 0 & D & 0 \\ 0 & -C & 0 & A \end{pmatrix}$$
$$= \begin{pmatrix} \alpha A & -\gamma C & \alpha C & \gamma A \\ -\beta B & \delta D & -\beta D & -\delta B \\ \alpha B & -\gamma D & \alpha D & \gamma B \\ \beta A & -\delta C & \beta C & \delta A \end{pmatrix}. \tag{29}$$

The same result holds if the substitutions be compounded in reverse order, so that the substitutions are commutative. Further, the only substitutions belonging to both of the sets (27) and (28) are seen to be

$$\xi_1' = \alpha\xi_1, \quad \eta_1' = \alpha\eta_1, \quad \xi_2' = \alpha\xi_2, \quad \eta_2' = \alpha\eta_2. \tag{30}$$

The substitution (27) leaves $\xi_1\eta_1 + \xi_2\eta_2$ absolutely invariant if and only if $\alpha\delta - \beta\gamma = 1$. Hence there are $(p^{2n} - 1)p^n$ such substitutions. It follows that there are

$$\{(p^{2n} - 1)p^n\}^2, \qquad (\text{if } p = 2)$$
$$\tfrac{1}{2}\{(p^{2n} - 1)p^n\}^2 \qquad (\text{if } p > 2)$$

distinct substitutions (29) for which

$$\alpha\delta - \beta\gamma = 1, \quad AD - BC = 1. \tag{31}$$

The substitution $T_{2,\kappa}$ will be of the form (29) only if

$$\alpha A = \delta D = 1, \quad \alpha D = \kappa, \quad \delta A = \kappa^{-1}, \quad \beta = \gamma = B = C = 0.$$

Therefore $A = \alpha^{-1}$, $D = \kappa\alpha^{-1}$, $\delta = \kappa^{-1}\alpha$, so that

$$\alpha\delta - \beta\gamma = \kappa^{-1}\alpha^2 \quad AD - BC = \kappa\alpha^{-2}.$$

It will thus satisfy the relations (31) only when κ is a square in the $GF[p^n]$. Hence there are at least $\{(p^{2n} - 1)p^n\}^2$ substitutions (29) which satisfy the single relation

$$(\alpha\delta - \beta\gamma)(AD - BC) = 1. \tag{32}$$

Among these does not occur the transposition $M_1 \equiv (\xi_1 \eta_1)$; for among the conditions that (29) shall reduce to M_1 are found

$$\alpha A = \delta D = 0, \quad \alpha D = \delta A = 1.$$

Since the group L_{2, p^n}, leaving $\xi_1\eta_1 + \xi_2\eta_2$, is of order $2\{(p^{2n}-1)p^n\}^2$, the group L'_{2, p^n} of the substitutions (29) which satisfy (32) is of index two under L_{2, p^n}. Further, the group L''_{2, p^n} of the substitutions (29) which satisfy (31) is of index 2 or 1 under L'_{2, p^n} according as $p > 2$ or $p = 2$. But L''_{2, p^n} has an invariant subgroup formed of the substitutions (27) which satisfy the relation $\alpha\delta - \beta\gamma = 1$. This subgroup, being simply isomorphic to the group of binary linear substitutions of determinant unity, is for $p = 2$, the group F_{1, p^n} of linear fractional substitutions of determinant unity on one index, but for $p > 2$ has the factor groups F_{1, p^n} and C, the latter being the group generated by the substitution changing the sign of every index. The quotient group of L''_{2, p^n} by the group of substitutions (27) is evidently F_{1, p^n}. Now F_{1, p^n} is *simple* if p^n is neither 2 nor 3.

Theorem:* *The factors of composition of* L_{2, p^n} *are*

(if $p > 2$) $\quad 2,\ 2,\ \frac{1}{2}(p^{2n}-1)p^n,\ \ \frac{1}{2}(p^{2n}-1)p^n,\ \ 2,$
(if $p = 2$) $\quad 2,\ (2^{2n}-1)2^n,\ \ (2^{2n}-1)2^n,$

except when $p_n = 2$ *or* 3, *when the composite numbers* 6 *and* 12 *respectively are to be replaced by their prime factors.*

51. Theorem: *For* $p^n > 3$, *the group* $G^{(3)}_{4, p^n}$, *leaving invariant*

$$\phi \equiv \zeta_1^2 + \zeta_2^2 + \zeta_3^2 + \nu\zeta_4^2, \qquad (\nu = \text{not-square})$$

is simply isomorphic to the group E_{4, p^n}, *leaving invariant*

$$f \equiv \xi_1\eta_1 + \xi_2\eta_2 + \lambda(\xi_1^2 + \eta_1^2),$$

where $\xi_1\eta_1 + \lambda\xi_1^2 + \lambda\eta_1^2$ *is irreducible in the* $GF[p^n]$.

---

*We readily verify the statement in §40 that, for $m = 2$, J_0 requires other generators than M_1M_2, $N_{1,2,\kappa}$. Indeed, every product derived from these two substitutions is of the form SM_1M_2, where S is derived from $N_{1,2,\kappa}$ and $R_{1,2,\kappa}$, each of which is of the form (27). Hence the group G generated by M_1M_2 and $N_{1,2,\kappa}$ is a subgroup of the group of substitutions (27) when extended by M_1M_2. Its order is therefore a factor of $2(2^{2n}-1)2^n$, and hence $< \{(2^{2n}-1)2^n\}^2$.

Suppose first that -1 is the square of a mark I belonging to the field. Then the substitution

$$\xi_2 = \zeta_1 + I\zeta_2, \quad \eta_2 = \zeta_1 - I\zeta_2,$$

transforms ϕ into

$$\phi_1 \equiv \xi_2\eta_2 + \zeta_3^2 + \nu\zeta_4^2.$$

Applying to ϕ_1 the substitution of determinant $2\alpha\beta$,

$$\zeta_3 = \alpha(\xi_1 - \eta_1), \quad \zeta_4 = \beta(\xi_1 + \eta_1), \tag{33}$$

we obtain the function

$$\xi_2\eta_2 + (2\nu\beta^2 - 2\alpha^2)\,\xi_1\eta_1 + (\alpha^2 + \nu\beta^2)(\xi_1^2 + \eta_1^2),$$

which may be made to assume the form f. Indeed, by §3, there exist $p^n + 1$ sets of solutions in the $GF[p^n]$ of

$$2\nu\beta^2 - 2\alpha^2 = 1.$$

At most, two of these sets of solutions make $\alpha\beta = 0$; for, $\alpha = 0$ gives a solution only when 2 is a not-square, in which case $\beta = 0$ is not a solution. Hence there are $p^n - 1$ substitutions (33) of determinant not zero which transform ϕ_1 into f

Suppose, however, that -1 is not a not-square in the field. We may take $\nu = -1$. Applying to ϕ the substitution of determinant $\alpha\beta$,

$$\zeta_1 = \alpha(\xi_1 - \eta_1), \quad \zeta_2 = \beta(\xi_1 + \eta_1), \quad \zeta_3 = \tfrac{1}{2}(\eta_2 + \xi_2), \quad \zeta_4 = \tfrac{1}{2}(\eta_2 - \xi_2),$$

we obtain the function

$$\xi_2\eta_2 + (2\beta^2 - 2\alpha^2)\,\xi_1\eta_1 + (\alpha^2 + \beta^2)(\xi_1^2 + \eta_1^2).$$

But there exist, in the $GF[p^n]$, $p^n - 1$ sets of solutions of

$$2\beta^2 - 2\alpha^2 = 1.$$

Two of these sets make $\alpha\beta = 0$. Hence there are $p^n - 3$ substitutions of determinant not zero which reduce ϕ to the form f.

For $p^n = 3$, there are no quadratic forms

$$q \equiv \xi_1\eta_1 + \lambda\xi_1^2 + \lambda\eta_1^2,$$

irreducible in the $GF[p^n]$. Indeed, according as $\lambda = +1$ or -1, q becomes $(\xi_1 - \eta_1)^2$ or $-(\xi_1 + \eta_1)^2$.

52. Denote by E'_{4, p^n} the subgroup which $M_1 \equiv (\xi_1 \eta_1)$ extends to the total group E_{4, p^n}. The order of E'_{4, p^n} is

$$(p^{3n} + p^n)(p^{2n} - 1)p^n \equiv (p^{4n} - 1)p^{2n}.$$

If $p = 2$, the group E'_{4, p^n} is identical with the second hypoabelian group $G_{\lambda'}$ on two pairs of indices. It will be evident from what follows that the group E'_{4, p^n}, for $p > 2$, has a subgroup E''_{4, p^n} of index two which is extended to E' by the substitution $T_{2, N}$, where N is a not-square in the $GF[p^n]$. We may verify this result directly. Thus, if -1 be a not-square, the substitution $T_{2, -1}$ of E' corresponds to the substitution

$$\zeta_3' = -\zeta_3, \quad \zeta_4' = -\zeta_4 \tag{34}$$

of the group $G^{(3)}_{4, p^n}$, leaving ϕ invariant. If -1 be the square of a mark I in the field, the substitution $T_{2, N}$ corresponds to the substitution of $G^{(3)}_{4, p^n}$,

$$\begin{cases} \zeta_1' = \quad \tfrac{1}{2} \ (N + N^{-1})\zeta_1 + \tfrac{1}{2} I(N - N^{-1})\zeta_2, \\ \zeta_2' = -\tfrac{1}{2} I(N - N^{-1})\zeta_1 + \tfrac{1}{2} \ (N + N^{-1})\zeta_2, \end{cases} \tag{35}$$

which is an orthogonal substitution, leaving $\zeta_1^2 + \zeta_2^2$ invariant, but not of the form $Q^{\alpha, \beta}_{1, 2}$ since

$$2\alpha^2 - 1 = \tfrac{1}{2}(N + N^{-1})$$

would require $\alpha^2 = (N + 1)^2/4N$, a not-square.

By §§15–17 the substitution (34) or (35) respectively serves to extend a subgroup H to $G^{(3)}_{4, p^n}$.

For $p = 2$, we set $E'' \equiv E'$.

53. Theorem: *The group E''_{4, p^n} is simply isomorphic to the group of linear fractional substitutions of determinant unity.*

We transform the invariant f into $XY + \xi_2\eta_2$ by means of the following substitution of determinant $2\sigma + 1$,

$$Z: \begin{cases} X = \lambda\xi_1 - \sigma\eta_1, \\ Y = \ \xi_1 - \lambda\sigma^{-1}\eta_1, \end{cases}$$

where σ is a root of the equation

$$\sigma^2 + \sigma + \lambda^2 = 0,$$

irreducible in the $GF[p^n]$ in virtue of the irreducibility of

$$(\lambda\xi_1)^2+(\lambda\xi_1)\eta_1+\lambda^2\eta_1^2.$$

For the reciprocal of Z we find

$$Z^{-1}:\ \begin{cases}(2\sigma+1)\xi_1=-\lambda\sigma^{-1}X+\sigma Y,\\ (2\sigma+1)\eta_1=-\qquad X+\lambda Y.\end{cases}$$

Every substitution S in the $GF[p^n]$, leaving f invariant, is transformed by Z into a substitution S', leaving $XY+\xi_2\eta_2$ invariant, but having its coefficients in the $GF[p^{2n}]$. In particular, Z transforms M_2 and $T_{2,N}$ into themselves. Hence Z transforms the group E''_{4,p^n}, which M_2 and $T_{2,N}$ extend to the total group, leaving f invariant, into a group K which is extended by M_2 and $T_{2,N}$ to the total group, leaving $XY+\xi_2\eta_2$ invariant. It follows from §50 that the substitutions of K are of the form (29), when operating on the indices X, Y, ξ_2, η_2, in which α, β, γ, δ, A, B, C, D are marks of the $GF[p^{2n}]$ satisfying the relations

$$\alpha\delta-\beta\gamma=1,\quad AD-BC=1. \tag{36}$$

Expressing the substitution (29) in terms of the indices ξ_1, η_1, ξ_2, η_2, it is seen to take the form:

$$\left\{\begin{array}{l}\xi_1'=\sum\limits_j^{1,2}(\alpha_{1j}\xi_j+\gamma_{1j}\eta_j),\quad \eta_1'=\sum\limits_j^{1,2}(\beta_{1j}\xi_j+\delta_{1j}\eta_j),\\ \xi_2'=(\lambda\alpha B-\gamma D)\xi_1-(\sigma\alpha B-\lambda\sigma^{-1}\gamma D)\eta_1+\alpha D\xi_2+\gamma B\eta_2,\\ \eta_2'=(\lambda\beta A-\delta C)\xi_1-(\sigma\beta A-\lambda\sigma^{-1}\delta C)\eta_1+\beta C\xi_2+\delta A\eta_2,\end{array}\right\} \tag{37}$$

where we have written for brevity

$$\begin{aligned}
\alpha_{11}&=(2\sigma+1)^{-1}(\sigma\delta D-\lambda\sigma\beta B+\lambda\sigma^{-1}\gamma C-\lambda^2\sigma^{-1}\alpha A),\\
\gamma_{11}&=(2\sigma+1)^{-1}(\lambda\alpha A-\lambda\delta D+\sigma^2\beta B-\lambda^2\sigma^{-2}\gamma C),\\
\beta_{11}&=(2\sigma+1)^{-1}(\gamma C+\lambda\delta D-\lambda\alpha A-\lambda^2\beta B),\\
\delta_{11}&=(2\sigma+1)^{-1}(\sigma\alpha A+\lambda\sigma\beta B-\lambda\sigma^{-1}\gamma C-\lambda^2\sigma^{-1}\delta D),\\
\alpha_{12}&=(2\sigma+1)^{-1}(-\sigma\beta D-\lambda\sigma^{-1}\alpha C),\quad \gamma_{12}=(2\sigma+1)^{-1}(-\sigma\delta B-\lambda\sigma^{-1}\gamma A),\\
\beta_{12}&=(2\sigma+1)^{-1}(-\alpha C-\lambda\beta D),\quad \delta_{12}=(2\sigma+1)^{-1}(-\gamma A-\lambda\delta B).
\end{aligned}$$

We next require that all of the coefficients of the substitution (37) shall belong to the $GF[p^n]$. The totality of substitutions thus obtained form the group K simply isomorphic to E''_{4,p^n}.

54. Since σ belongs to the $GF[p^{2n}]$, but not to the $GF[p^n]$, we may set

$$\alpha = a + a'\sigma, \quad \beta = b + b'\sigma, \quad \gamma = c + c'\sigma, \quad \delta = d + d'\sigma.$$

The coefficient δA must belong to the $GF[p^n]$. If $d' \neq 0$, we may set $A = \varkappa + A_1 d'\sigma$, where $\varkappa$ and A_1 are marks of the $GF[p^n]$. Applying $\sigma^2 + \sigma + \lambda^2 = 0$, we find

$$\delta A = (\varkappa d - \lambda^2 A_1 \overset{2}{d'}) + \sigma(\varkappa + dA_1 - A_1 d')\, d'.$$

Hence must $\varkappa = A_1 d' - dA_1$. If $d' = 0$, $d \neq 0$, we may evidently set $A = -dA_1$, a mark of the field. Finally, if $d = d' = 0$, so that $\delta = 0$, the coefficients of ξ_1 and η_1 in η_2' require that $\lambda\beta A$ and $-\sigma\beta A$ be marks of the $GF[p^n]$ and hence require that $\beta A = 0$. Since $\alpha\delta - \beta\gamma \neq 0$, we must have $\beta\gamma \neq 0$ and therefore $A = 0$. Hence in every case we may set $A = (d' - d + d'\sigma)\, A_1$.

Also γB, βC, δA must belong to the $GF[p^n]$. Proceeding as before, we find that we may set

$$A = (d' - d + d'\sigma)\, A_1, \quad B = (c' - c + c'\sigma)\, B_1,$$
$$C = (b' - b + b'\sigma)\, C_1, \quad D = (a' - a + a'\sigma)\, D_1,$$

where A_1, B_1, C_1 and D_1 belong to the $GF[p^n]$.

We next set up the conditions that the remaining coefficients of the substitution (37) shall belong to the $GF[p^n]$. Expressing the coefficients $\lambda\beta A - \delta C$ and $-\sigma\beta A + \lambda\sigma^{-1}\delta C$ in the form $R + S\sigma$ and setting the coefficient of σ equal zero, we obtain respectively

$$(b'd - bd')(\lambda A_1 + C_1) = 0, \quad (bd - b'd + \lambda^2 b'd')(\lambda A_1 + C_1) = 0.$$

Hence either $\lambda A_1 + C_1 = 0$ or else $\delta C = \beta A = 0$. Consider the latter alternative. If $\delta \neq 0$, then $C = 0$, and therefore $A \neq 0$, since $AD - BC \neq 0$. Hence $\beta = 0$, i. e. $b = b' = 0$. We may therefore give to C_1 an arbitrary value in the $GF[p^n]$ and in particular a value making $\lambda A_1 + C_1 = 0$. If, however, $\delta = 0$, an arbitrary value in the field may be assigned to A_1, so that again we may take $\lambda A_1 + C_1 = 0$. Hence, in every case, $\lambda A_1 + C_1 = 0$.

By a simple interchange of letters, it follows that the coefficients $\lambda\alpha B - \gamma D$ and $-\sigma\alpha B + \lambda\sigma^{-1}\gamma D$ will belong to the $GF[p^n]$ if and only if $\lambda B_1 + D_1 = 0$.

In order that $(2\sigma+1)^{-1}(R+\sigma S)$ shall belong to the $GF[p^n]$, when R and S do, it is necessary and sufficient that $S=2R$. Hence the coefficients denoted by δ_{12} and γ_{12} will belong to the field if and only if respectively

$$(A_1+\lambda B_1)(2cd+2c'd'\lambda^2-c'd-cd')=0,$$
$$(A_1+\lambda B_1)[cd-cd'+c'd'\lambda^2-2\lambda^2(c'd-cd')]=0.$$

If $A_1+\lambda B_1\neq 0$, we find the relation $(c'd-cd')(1-4\lambda^2)=0$. But, for $p>2$, $\lambda\neq\frac{1}{2}$, since then $\sigma^2+\sigma+\lambda^2=(\sigma+\frac{1}{2})^2$. Hence

$$c'd-cd'=0,\quad cd-cd'+c'd'\lambda^2=0,$$

so that $\gamma A=\delta B=0$. By the reasoning given above, we may assume that, in every case, $A_1+\lambda B_1=0$.

If we consider the coefficients α_{12} and β_{12}, a simple interchange of letters gives the result $C_1+\lambda D_1=0$ as the condition that α_{12} and β_{12} belong to the $GF[p^n]$.

We have now obtained the following results:

$$C_1=-\lambda A_1,\quad B_1=-\lambda^{-1}A_1,\quad D_1=A_1. \tag{38}$$

In virtue of these relations we may verify that the coefficients α_{11}, γ_{11}, β_{11}, δ_{11} belong to the $GF[p^n]$. The conditions for β_{11} and δ_{11} are respectively

$$(2bc+2\lambda^2b'c'-b'c-bc')(C_1-\lambda^2B_1)$$
$$+(2ad+2\lambda^2a'd'-a'd-ad')(\lambda D_1-\lambda A_1)=0,$$
$$[a'd-ad-\lambda^2a'd'+2\lambda^2(ad'-a'd)][A_1-D_1]$$
$$+[cb'-cb-\lambda^2c'b'+2\lambda^2(c'b-cb')][\lambda B_1-\lambda^{-1}C_1]=0.$$

As to the coefficients α_{11} and γ_{11}, we observe that

$$\gamma_{11}+\beta_{11}=(2\sigma+1)^{-1}(1-\lambda^2\sigma^{-2})(\gamma C+\sigma^2\beta B)=\sigma^{-1}(\gamma C+\sigma^2\beta B),$$
$$\alpha_{11}+\delta_{11}=(2\sigma+1)^{-1}(\sigma-\lambda^2\sigma^{-1})(\alpha A+\delta D)\quad=\alpha A+\delta D.$$

These sums will belong to the $GF[p^n]$ if respectively

$$(b'c-bc-\lambda^2b'c')(B_1-\lambda^{-2}C_1)=0,\quad (a'd-ad')(D_1-A_1)=0.$$

55. The condition $\alpha\delta-\beta\gamma=1$ requires that

$$\begin{cases} ad-bc-\lambda^2a'd'+\lambda^2b'c'=1, \\ ad'+a'd-a'd'=bc'+b'c-b'c'. \end{cases} \tag{39}$$

In virtue of these relations we find that

$$AD - BC = (\sigma + 1)(a'd' - ad' - a'd)(A_1D_1 - B_1C_1) + (ad - \lambda^2 a'd')(A_1D_1 - B_1C_1) + B_1C_1.$$

Applying (38), we find

$$AD - BC = B_1C_1 = A_1^2.$$

Hence, from (36), $A_1 = \pm 1$.

But the substitution (29) is unaltered by a simultaneous change of sign in $a, a', b, b', c, c', d, d'$. Hence we may set

$$A_1 = +1, \quad C_1 = -\lambda, \quad B_1 = -\lambda^{-1}, \quad D_1 = 1.$$

It follows that every substitution (29) of the group K is the product UV of two substitutions

$$U \equiv \begin{bmatrix} a + a'\sigma & 0 & 0 & c + c'\sigma \\ 0 & d + d'\sigma & -(b + b'\sigma) & 0 \\ 0 & -(c + c'\sigma) & a + a'\sigma & 0 \\ b + b'\sigma & 0 & 0 & d + d'\sigma \end{bmatrix},$$

$$V \equiv \begin{bmatrix} d' - d + d'\sigma & 0 & -\lambda(b' - b + b'\sigma) & 0 \\ 0 & a' - a + a'\sigma & 0 & \lambda^{-1}(c' - c + c'\sigma) \\ -\lambda^{-1}(c' - c + c'\sigma & 0 & a' - a + a'\sigma & 0 \\ 0 & \lambda(b' - b + b'\sigma) & 0 & d' - d + d'\sigma \end{bmatrix},$$

the coefficients of which must satisfy the relations (39). Now U and V are com mutative and are identical only when each is the identity. Hence the group of the products UV is isomorphic to the group of the substitutions U. For $p > 2$ the isomorphism is (1, 2); indeed, a change of sign of a, a', etc., alters U but not the product UV; while, further, UV is the identity only when

$$B = C = \beta = \gamma = 0, \quad A = D, \quad \alpha = \delta, \quad \alpha A = 1,$$

whence $\alpha = \delta = A = D = \pm 1$, giving two [distinct if $p > 2$] substitutions U. By §50 the group of the substitutions U has (1, 2) isomorphism if $p > 2$, but simple isomorphism if $p = 2$, with the group F_{1, p^n} of linear fractional substitutions of determinant unity. Hence the group K of the substitutions UV, and therefore the group E''_{4, p^n}, is simply isomorphic to the simple group F_{1, p^n}.

56. We conclude with a summary of the simple groups obtained—

$(2^{nm}-1)[(2^{2n(m-1)}-1)\,2^{2n(m-1)}]\ \ldots\ [(2^{2n}-1)\,2^{2n}].$ $(m>2)$

$(2^{nm}+1)[(2^{2n(m-1)}-1)\,2^{2n(m-1)}]\ \ldots\ [(2^{2n}-1)\,2^{2n}].$ $(m>1)$

$\frac{1}{2}(p^{n(m-1)}-1)\,p^{n(m-2)}(p^{n(m-3)}-1)\,p^{n(m-4)}\ \ldots\ (p^{2n}-1)\,p^{n},$
$(p>2,\ m$ odd and >1; exception $p^n=3,\ m=3)$.

$\frac{1}{4}[p^{n(m-1)}-\varepsilon^{\frac{m}{2}}p^{n(\frac{m}{2}-1)}](p^{n(m-2)}-1)\,p^{n(m-3)}\ \ldots\ (p^{2n}-1)\,p^{n},$
$(p>2,\ m$ even and $>4)$.

$\frac{1}{2}[p^{n(m-1)}+\varepsilon^{\frac{m}{2}}p^{n(\frac{m}{2}-1)}](p^{n(m-2)}-1)\,p^{n(m-3)}\ \ldots\ (p^{2n}-1)\,p^{n},$
$(p>2,\ m$ even and $>2)$.

Here $\varepsilon=\pm 1$ according as p^n is of the form $4l\pm 1$. The first and second sets are obtained from the first and second hypoabelian groups; the third and fourth sets from the orthogonal group, and the fifth set from the group $G^{(m-1)}_{m,\,p^n}$.

UNIVERSITY OF CALIFORNIA, *December* 30, 1898.